

هوشمند
هشیار
قوی
مهربان
شجاع

به برنامه آموزشی **Be Internet Awesome**، محصول مشترک گوگل، **The Net Safety Collaborative** و **Internet Keep**، **Safe Coalition** خوش آمدید. این برنامه آموزشی بخشی از برنامه **Be Internet Awesome** است و هدف از طراحی آن کمک به آموزش مهارت‌هایی است که به منظور ایمن‌سازی و هوشمند سازی کودکان در محیط‌های آنلاین به آنها نیاز است.

در سال جاری 10 فعالیت جدید به این برنامه درسی اضافه شد. ما با همکاری سازمان غیرانتفاعی کارگروه کودکان، فعالیت‌های یادگیری اجتماعی-هیجانی جدیدی را طراحی کردیم که کودکان را در حین گشت و گذارهای اینترنتی خود راهنمایی می‌کنند. علاوه بر این مطالب درسی جدیدی در مورد سواد جستجو اضافه کرده‌ایم و فعالیت‌های ایمنی و امنیتی خود را به منظور پاسخگویی به نیازهای دنیای دیجیتال امروزی به روزرسانی کردیم. این برنامه درسی شامل فعالیت‌هایی است که برای سطوح خاصی طبقه‌بندی شده‌اند و طیف وسیعی از سیر تکاملی کودکان را در خود جای می‌دهند.

نکته مهمی که باید به آن اشاره کنیم این است که برنامه **Be Internet Awesome** توسط مرکز پژوهشی جرایم علیه کودکان دانشگاه نیوهمپشایر مورد ارزیابی کامل قرار گرفته است و در نتیجه این مطالعه مشخص شد این برنامه اولین برنامه ایمنی در اینترنت است که تأثیر مثبتی بر یادگیری موضوعات ایمنی آنلاین و شهروندی دیجیتال دانش‌آموزان دارد.

برنامه درسی **Be Internet Awesome** برنامه‌ای جامع و مستقل است و تمام فعالیت‌های مندرج در آن به گونه‌ای طراحی شده‌اند که بدون هیچ دانش تخصصی پیش نیاز و با حداقل آمادگی کلاسی و بدون نیاز به تجهیزات یا منابع خاص آموزشی قابل استفاده هستند. همچنین مطالب درسی مندرج در این برنامه با استفاده از محیط بازی اینترنتی که یک بازی آنلاین ماجراجویی با هدف یادگیری ایمنی دیجیتالی و شهروندی به شکلی تعاملی و سرگرم‌کننده؛ درست مانند اینترنت؛ است، توسعه یافته است.

Internet Code of Awesome پیرامون پنج موضوع اصلی شهروندی دیجیتال و ایمنی قرار دارد:

- با احتیاط به اشتراک بگذارید:** ردپای دیجیتالی و ارتباطات مسئولانه
- به دام کلاهبرداران نیفتید:** فیشینگ، کلاهبرداری و منابع معتبر
- اطلاعات شخصی خود را محرمانه نگه دارید:** امنیت آنلاین و رمزهای عبور
- مهربانی، زیبا است:** مبارزه با رفتارهای منفی آنلاین
- موارد مشکوک را به دقت بررسی کنید:** محتواها و سناریوهای مشکوک

این برنامه درسی برای کلاس‌های دوم تا ششم طراحی شده است، با این حال معلمان کلاس‌های بالاتر یا پایین‌تر می‌توانند از مزایای این دروس برای دانش‌آموزان خود بهره‌مند شوند، بویژه در زمینه واژگان کلیدی، مباحث کلاسی (سنین کمتر یا بیشتر) و محیط بازی. ما می‌خواهیم خودتان بهترین کار را برای دانش‌آموزان خود انجام دهید، چه این کار تکمیل برنامه درسی از ابتدا تا انتها باشد، یا بسنده کردن به یک یا دو موضوع درسی که بیش از دیگر مطالب مورد نیاز دانش‌آموزان شما است. با تکمیل برنامه درسی به منابع آموزشی و خانوادگی بیشتری دست خواهید یافت، منابعی همچون اسلایدهای آماده تدریس **Pear Deck**، فعالیت‌های قابل چاپ و دستورالعمل‌ها و نکاتی برای خانواده و اجرا در منزل.

انجمن بین‌المللی فناوری در آموزش (**ISTE**) به ارزیابی مستقل برنامه **Be Internet Awesome** پرداخته است و این برنامه را به عنوان منبعی برای آماده سازی دانش‌آموزان در سنین ابتدایی در جهت دستیابی به استانداردهای **ISTE** شناسایی کرده است. **ISTE** به این برنامه آموزشی نشان همسویی در آماده سازی را اعطاء کرده است.



4	راهنمای مربی منبع 1: نحوه آموزش برنامه آموزشی منبع 2: فعالیت‌های واژگانی منبع 3: نمونه پست الکترونیکی / نامه معرفی برنامه به والدین منبع 4: پرسش‌های متداول
---	--

8	بخش 1 با احتیاط به اشتراک بگذارید درس 1: چه موقع نباید اطلاعات خود را به اشتراک گذاشت درس 2: محرمانه نگه داشتن اطلاعات. درس 3: منظورم این نبود! درس 4: کادربندی کنید. درس 5: او چه کسی است؟ درس 6: دیگران چگونه از آنلاین بودن ما با خبر می‌شوند؟ درس 7: اینترلند: کوهستان هوشیار
---	---

20	بخش 2 به دام کلاهبردارها نیفتید درس 1 پنجره‌های پاپ‌آپ، کت فیشینگ و سایر کلاهبرداری‌ها. درس 2: مخاطب من چه کسی است؟ درس 3: آیا این واقعا درست است؟ درس 4: تشخیص اطلاعات آنلاین نامطمئن درس 5: اگر یک موتور جستجو بودیم! درس 6: تمرین جستجوی اینترنتی درس 7: اینترلند: رودخانه واقعیت
----	--

38	بخش 3 اطلاعات شخصی خود را محرمانه نگه دارید درس 1 : این که من نبودم! درس 2 : چگونه یک رمز عبور مطمئن بسازیم درس 3: در حفظ اسرار خود کوشا باشید درس 4 : اینترلند: برج گنج
----	---

46	بخش 4 مهربانی، زیبا است درس 1.1: درک احساسات درس 1.2: تمرین همدلی درس 2.2: روش‌های نشان دادن محبت درس 3: از بد به خوب درس 4: لحن سخن گفتن شما درس 5: کلمات چگونه می‌توانند تصویر کلی را تغییر دهند درس 6: اینترلند: قلمروی مهربانی
----	--

بخش 5 موارد مشکوک را به دقت بررسی کنید

- درس 1: شجاع بودن به چه معنا است؟
- درس 2: از نظاره‌گر تا یاری‌رسان
- درس 3: یاری‌رسان‌ها اختیاراتی دارند!
- درس 4.1: مشاهده موضوعات ناراحت کننده: چه باید کرد؟
- درس 4.2: موضوعات ناراحت کننده آنلاین: چه باید کرد؟
- درس 5.1: در صورت مشاهده موارد ناپسند بر روی صفحه نمایش چه باید کرد؟
- درس 5.2: کنترل سوءرفتارهای آنلاین
- درس 6: چه زمان باید از دیگران کمک خواست
- درس 7: آن را به صورت آنلاین هم گزارش دهید

راهنمای مربی: منبع 1

نحوه تدریس برنامه آموزشی

برنامه آموزشی

Be Internet Awesome طراحی انعطاف‌پذیری دارد، بنابراین می‌توانید به آسانی آن را برای دانش‌آموزان در کلاس اجرا کنید. بسته به برنامه زمانی و میزان آمادگی دانش‌آموزان، می‌توانید هر یک از دروس مندرج در برنامه آموزشی را در صورت نیاز تغییر دهید. به طور مثال ممکن است در درسی از شما خواسته باشیم فعالیتی را برای کل کلاس برگزار کنید، اما با شناختی که از دانش‌آموزان خود دارید، ممکن است احساس کنید اگر دانش‌آموزان فعالیت مذکور را در گروه‌های کوچک‌تر انجام دهند، عملکرد بهتری خواهند داشت. این‌ها ترفندهایی هستند که امیدواریم توانمندی انجام آنها را داشته باشید. این همان جادوی معلم است.



نکاتی در مورد برنامه آموزشی:

- در هر بخش فهرست واژگانی وجود دارد که در کل درس به کار برده می‌شوند. می‌توانید این فهرست را چاپ کنید و به عنوان منبع در اختیار دانش‌آموزان خود قرار دهید. حتماً فعالیت‌های واژگانی را که در صفحات بعدی ارائه کرده‌ایم، بررسی کنید!
- هر یک از پنج بخش این برنامه آموزشی از دروس متفاوتی تشکیل شده است و پیکربندی هر درس به ترتیب زیر است:
 - ✓ **اه داف درس برای دانش‌آموزان.**
 - ✓ **بیابید حرف بزیم:** دانش پیش زمینه برای معلمان که به زبانی ساده و قابل فهم برای دانش‌آموزان نوشته شده است (در صورتی که بخواهید فقط آن را برای دانش‌آموزان خود بخوانید).
 - ✓ **فعالیت:** برخی فعالیت‌ها ممکن است برای سطوح تحصیلی خاصی پیشنهاد شوند.
 - ✓ **آموزه‌ها:** خلاصه محتوای درس و فرصتی برای تفکر.
- در کنار هر یک از عناوین درسی علامتی به منظور نشان دادن سطح تحصیلی مناسب درج شده است. همچنین اگر درس در زمینه سواد رسانه‌ای و/یا یادگیری اجتماعی-عاطفی باشد، علامت مخصوص در کنار درس درج شده است.

SEL	ML	4-6	2-3	2-6
یادگیری اجتماعی عاطفی	سواد رسانه‌ای	پایه 4-6	پایه 2-3	پایه 2-6

4. این برنامه آموزشی به گونه‌ای طراحی شده است که بتوان آن را به دو روش مختلف تدریس کرد: روش اول تدریس به همان ترتیبی است که دروس ظاهر می‌شوند و روش دوم تدریس به ترتیبی است که با نیازهای یادگیری دیجیتالی خاص دانش‌آموزان مطابقت داشته باشد. هر یک از واحدها به شکلی هدفمند برای کلاس‌های درس از ابتدا تا انتها طراحی شده است، اما بسیاری از دانش‌آموزان ابتدایی با دانش پایه این روند آشنایی دارند و می‌توانند به شما کمک کنند مهارت‌های خاصی که می‌خواهند یا باید توسعه دهند را کشف کنید. با دانش‌آموزان خود در مورد کارهایی که انجام می‌دهند و نمی‌دانند نقطه مناسبی برای شروع خواهد بود، صحبت کنید. امیدواریم همگی شما از این برنامه آموزشی لذت ببرید.

راهنمای مربی: منبع 2

فعالیت‌های واژگانی

واژگان مورد استفاده در این فعالیت‌ها را می‌توان در ابتدای هر بخش درسی یافت.

• بیابید حرف بز نیم:



وسایل مورد نیاز:

تابلویی برای نشان دادن
واژگان تخته سیاه، مقوا، وایت بورد
و از این قبیل

دستورالعمل‌ها:

1. هر دانش‌آموز شریکی پیدا کند.
2. شریک 1 پشت به تخته کلاس بایستد. (دانش‌آموز می‌تواند بنشیند یا بایستد)
3. آموزگار سه تا پنج کلمه را روی تخته کلاس بنویسد.
4. شریک 2 روبروی تخته کلاسی ایستاده و اولین واژه را بدون ذکر صریح آن برای شریک 1 توضیح دهد.
5. شریک 1 سعی کند واژه را حدس بزند.
6. در صورتی که شریک 1 اولین واژه را به درستی حدس زد، شریک 2 به سراغ واژه بعدی برود.
7. مراحل 3-6 را ادامه دهید تا شریک 1 تمام واژگان نوشته شده روی تخته را حدس بزند.
8. در دور بعدی شریک 1 و 2 باید نقش خود را تغییر دهند. این فعالیت را با واژگان جدید تکرار کنید

• بینگو:



وسایل مورد نیاز:

کارت‌های بینگوی
قطعات بازی (هر چیزی که بتوان از آن برای
علامت‌گذاری استفاده کرد، مکعب‌های
کوچک، گیره‌های کاغذی، لوبیا و از این
قبیل)

دستورالعمل‌ها:

1. کارت‌های بینگوی (کارت‌های 5x5 و یا 3x3) و قطعات بازی را بین دانش‌آموزان تقسیم کنید.
2. دانش‌آموزان کارت‌های خود را با واژگان مندرج در یکی از بخش‌های مشخص تکمیل کنند.
3. آموزگار تعریف مربوط به یکی از واژگان را می‌خواند.
4. دانش‌آموزان به جستجو پرداخته تا ببینند آیا کلمه‌ای مطابق با تعریف آموزگار روی کارت آنها وجود دارد یا خیر و اگر چنین باشد یکی از قطعات بازی را روی آن می‌گذارند.
5. وقتی دانش‌آموز کارت بازی خود را به شکل عمودی، افقی یا مورب با قطعات بازی تکمیل کرد می‌تواند با گفتن عبارت «بینگو» این موضوع را اعلام کند.
6. به بازی با کارت‌های بینگو ادامه دهید یا از دانش‌آموزان بخواهید قطعات بازی را از روی کارت برداشته و دوباره بازی کنند.

• شبکه واژگان:



وسایل مورد نیاز:

کارت شبکه واژگان (صفحه 8 توزیع شود)

دستورالعمل‌ها:

1. هر دانش‌آموز یک شریک پیدا کند.
2. کارت‌های شبکه واژگان را بین هر گروه توزیع کنید (دانش‌آموزان می‌توانند تصویر کارت‌های شبکه واژگان را بر روی کاغذ بکشند).
3. دانش‌آموزان یک واژه را درون دایره مندرج بر روی کارت می‌نویسند. می‌توانید این مرحله را به سه روش مختلف اجرا کنید:
 - واژه یکسانی را برای تمامی گروه‌ها اختصاص دهید.
 - به هر گروه یک کلمه متفاوت دهید.
 - دانش‌آموزان واژگان خود را از فهرستی واحد انتخاب کنند.
4. دانش‌آموزان با شریک خود کارت را تکمیل می‌کنند.
5. پس از تکمیل کارت‌ها، چندین راه وجود دارد که بدان طریق فعالیت را گسترش دهید:
 - دانش‌آموزان برای یک کلمه جدید، کارت کلمات شبکه واژگان دیگری را تکمیل می‌کنند.
 - کارت‌های تکمیل شده را جمع‌آوری کنید و روی دیوار مخصوص نصب کنید.
 - یک بازدید کلاسی ترتیب دهید تا تمام دانش‌آموزان بتوانند کارت‌های شبکه واژگان هم‌کلاسی‌های خود را بخوانند.

ادامه در صفحه بعد ←

توزیع شود: منبع 2
کارت بینگو 5x5

توزیع شود: منبع 2

کارت بینگو 3x3

الگوی پست الکترونیکی / نامه معرفی والدین

آموزان خود اطلاع دهید که شما از برنامه آموزشی توانید به آن وسیله به والدین دانش در این قسمت یک نمونه پست الکترونیکی یا نامه وجود دارد که می - استفاده می کنید تا به فرزندانشان در راستای تبدیل شدن به شهروندان دیجیتالی باهوش و ایمن، کمک کنید.

والدین گرامی:

وقتی فرزندان ما کوچک هستند تلاش می کنیم بتوانند بهترین استفاده را از اینترنت برده و در عین حال آنها را در دنیای اینترنت ایمن نگه داریم. با هرچه بزرگتر شدن کودکان، نقش ما در راستای این یاری رسانی تغییر می کند و تلاش می کنیم فرزندانمان، خود یاد بگیرند که با خیالی راحت و با استفاده از تفکر و اندیشه خود بخش های دیجیتالی زندگی خود را هدایت کنند.

در [نام مدرسه]، ما به مشارکت با والدین باور داشته و دانش آموزان کلاس (پایه کلاسی) خود را برای موارد زیر آماده می کنیم:

تفکر انتقادی داشته باشند و برنامه ها، وب سایت ها و دیگر محتواهای دیجیتال را ارزیابی کنند.
از خود در برابر تهدیدات آنلاین، از جمله زورگویی و کلاهبرداری محافظت کنند.
در به اشتراک گذاردن مطالب، هوشمندانه عمل کنند: چه چیز، چه زمان، چگونه و با چه کسی!
با سایر افراد در فضای آنلاین مهربان بوده و محترمانه رفتار کنند، از جمله به حریم خصوصی دیگران احترام بگذارند.
در موقعیت های دشوار از والدین یا بزرگسالان مورد اعتماد خود کمک بخواهند.

در سال تحصیلی جاری این تلاش ها برنامه آموزشی را نیز شامل شده است. این برنامه، برنامه ای چند وجهی است که برای آموزش مهارت هایی که فرزندان ما در راستای حفظ ایمنی و هوشمندی آنلاین خود به آنها نیاز دارند طراحی شده است. اینترنت که یکی از منابع مندرج در این برنامه است یک بازی مبتنی بر مرورگر است که باعث می شود یادگیری چنین مهارت هایی تعاملی تر و سرگرم کننده تر باشد. می توان این بازی را در خانه نیز انجام داد فرزند شما ممکن است دوست داشته باشد به شما نشان دهد که چگونه این کار را انجام می دهد. این برنامه که با همکاری گوگل با مربیان، پژوهشگران و متخصصین امنیت آنلاین در و توسعه یافته است تجارب یادگیری سرگرم کننده و متناسب سن را ارائه می دهد که پیرامون پنج مبحث اصلی قرار دارند:

- با احتیاط به اشتراک بگذارید.

- به دام کلاهبردارها نیفتید.

- اطلاعات شخصی خود را محرمانه نگه دارید.

- مهربانی، زیبا است.

- موارد مشکوک را به دقت بررسی کنید.

خوشحال خواهیم شد اگر بتوانیم اطلاعات بیشتری در مورد این برنامه جدید با شما به اشتراک بگذاریم، از جمله معرفی برخی منابع که دانش آموز از آنها در کلاس استفاده خواهد کرد، همچنین از شما دعوت می کنیم منابع مندرج در وبسایت را مطالعه کنید. از شما می خواهیم از فرزند خود در مورد آنچه که در حال یادگیری آن است، پرس و جو کرده و این گفتگو را در خانه نیز ادامه دهید، و چه کسی می داند، ممکن است خودتان نیز چند ترفندی برای حفظ حریم خصوصی و امنیت خود یاد بگیرید.

با تشکر

[نام شما]

پرسش‌های متداول

آیا ضروری است قبل از این که دانش‌آموزان بازی در اینترنت را شروع کنند، کل دروس تدریس شوند؟

خیر، اما می‌تواند مفید باشد. بهترین زمان برای بازی وقتی است که بازی باعث تقویت آموزه‌های برنامه آموزشی شود و همچنین زمانی که دانش‌آموزان از این فرصت برخوردار باشند که قبل از شروع بازی در مباحث و ایده پردازی‌ها مشارکت داشته باشند. در این صورت بازی سرگرم‌کننده‌تر خواهد بود.

آیا دانش‌آموزان برای استفاده از برنامه آموزشی به حساب کاربری گوگل نیاز دارند؟

خیر! در دسترس تمام افراد است. از آنجاییکه گوگل هیچ داده دانش‌آموزی را جمع‌آوری نمی‌کند، به هیچ‌گونه لاگین کردن، گذرواژه و یا پست الکترونیکی نیاز ندارد. در به اشتراک گذاردن مطالب، هوشمندانه عمل کنید: چه چیز، چه زمان، چگونه و با چه کسی! با سایر افراد در فضای آنلاین مهربان بوده و محترمانه رفتار کنید، از جمله به حریم خصوصی دیگران احترام بگذارند. در موقعیت‌های دشوار از والدین یا بزرگسالان مورد اعتماد خود کمک بخواهند.

چه دستگاه‌هایی با اینترنت سازگار هستند؟

اینترنت بر روی هر دستگاهی که قابلیت اتصال به اینترنت و مرورگر را داشته باشد، قابل اجرا است. این بدان معناست که اغلب رایانه‌های رومیزی یا لپ‌تاپ‌ها، تبلت یا تلفن‌های همراه از قابلیت اجرای این برنامه برخوردار هستند.

آدرس سایت چیست؟

برای مشاهده صفحه اصلی این برنامه به آدرس اینترنتی visit.g.co/BelInternetAwesome مراجعه کنید. برای بازی اینترنتی به آدرس اینترنتی visit.g.co/Interland و برای پیاده‌سازی برنامه آموزشی Be Internet Awesome به آدرس اینترنتی g.co/BelInternetAwesomeEducators مراجعه کنید. برای دسترسی به منابع خانوادگی به آدرس اینترنتی g.co/BelInternetAwesomeFamilies مراجعه شود.

آیا برای آموزش برنامه آموزشی به آموزش خاصی نیاز داریم یا باید معلم خاصی باشیم؟

اولاً هر یک از معلمین پایه‌های اول تا دوازدهم می‌توانند این برنامه درسی را به دانش‌آموزان خود آموزش دهند. به هیچ آموزش اضافی لازم نیست.
دوماً هر معلمی، خاص است.
سوماً دروس مندرج در این برنامه به منظور درک متقابل دانش‌آموز و معلم به شیوه‌ای سرگرم‌کننده و ساده بهینه‌سازی شده‌اند و معلم در این ارتباط بایستی نقش شنونده فعال، بدون هیچ‌گونه داوری و قضاوتی را بازی کند.

این برنامه مناسب کدام یک از پایه‌های تحصیلی است؟

برنامه کامل که شامل برنامه آموزشی، بازی و منابع موجود در وبسایت است برای کاربران پایه‌های دوم تا ششم (سنین 7 تا 12 سال) طراحی شده است. با این حال، بسته به شیوه تنظیم برنامه آموزشی توسط آموزگار، موضوعات می‌توانند برای هر پایه‌ای مفید باشند.

این بازی چه نقشی در آموزش دانش‌آموزان دارد؟

بازی این فرصت را در اختیار دانش‌آموزان قرار می‌دهد تا به شکلی آزادانه شیوه‌های دیجیتالی سالم را کشف کرده و تعاملات دیجیتالی را در فضایی آموزشی و ایمن درک کنند و از این طریق باعث بهبود و تقویت مفاهیم برنامه آموزشی می‌شود.

آیا می‌توان دروس را در گوگل کلاس‌روم استفاده کرد؟

بله، صد در صد! شما می‌توانید اینترنت را به کلاس‌ها یا بخش‌های خاص اختصاص دهید و یا منبع را در قالب یک اعلامیه کلاسی در دسترس همه دانش‌آموزان خود قرار دهید.

آیا پوشه (فولدر) یا وبسایت مشترکی وجود دارد که کاربرگ‌های لازم به منظور نمایش بر روی تخته کلاس در آنها قابل دسترسی باشد؟

بله، این کاربرگ‌ها در قالب پاورپوینت وجود دارند. ما با Pear Deck کار کردیم تا توزیع و اشتراک‌گذاری برنامه آموزشی در قالب پاورپوینت آسان‌تر باشد. می‌توانید این قالب‌ها را در آدرس اینترنتی g.co/BeInternetAwesomeEducators پیدا کنید.

آیا به منظور استفاده از این برنامه باید در زمینه شهروندی دیجیتال تخصص داشته باشیم؟

خیر. این برنامه آموزشی به گونه‌ای طراحی شده است که هر معلمی قادر است به راحتی آن را کلاس تدریس کند. با این حال اگر به یادگیری هر چه بیشتر در زمینه امنیت دیجیتالی و موضوعات شهروندی علاقمند هستید، می‌توانید در دوره آنلاین ما برای مربیان به آدرس اینترنتی g.co/OnlineSafetyEduTraining شرکت کنید.

آیا برنامه درسی Be Internet Awesome با استانداردهای ملی یا ایالتی مطابقت دارد؟

از این که این موضوع برایتان مهم است، خوشحال هستیم. بله، همینطور است. برنامه درسی با استانداردهای ISTE (انجمن بین‌المللی فناوری در آموزش) و AASL (انجمن کتابداران مدارس آمریکا) مطابقت دارد.

آیا دانش‌آموزان می‌توانند کار خود را ذخیره کنند؟

این امکان در نسخه فعلی وجود ندارد و احتمالاً در نسخه‌های بعدی نیز چنین قابلیت اضافه نخواهد شد. این برنامه هیچ اطلاعات قابل شناسایی شخصی را به صورت فایل‌های ذخیره شده تولید یا ذخیره نمی‌کند. دلایل هدفمندی برای این کار وجود دارد. ما داده‌های دانش‌آموزی را جمع‌آوری نمی‌کنیم، و می‌خواهیم این تجربه برای همگان قابل دسترسی باشد، بنابراین نیازی به داشتن حساب کاربری، ورود به سیستم یا رمز عبور نیست.

این خیلی خوب است، اما خیلی از دانش‌آموزان من از این که بازی را به پایان رسانده‌اند و به خاطر مطالبی که یاد گرفته‌اند، به خود افتخار می‌کنند.

ما با شما هم عقیده هستیم و به همین دلیل یک گواهینامه قابل تنظیم ایجاد کرده‌ایم تا بتوانید نام دانش‌آموز خود را در آن وارد کنید و یک گواهی تکمیل دوره شخصی قابل چاپ برای دانش‌آموزان خود ایجاد کنید.

از کجا می‌توانم به سایر منابع آموزشی دست یابم؟

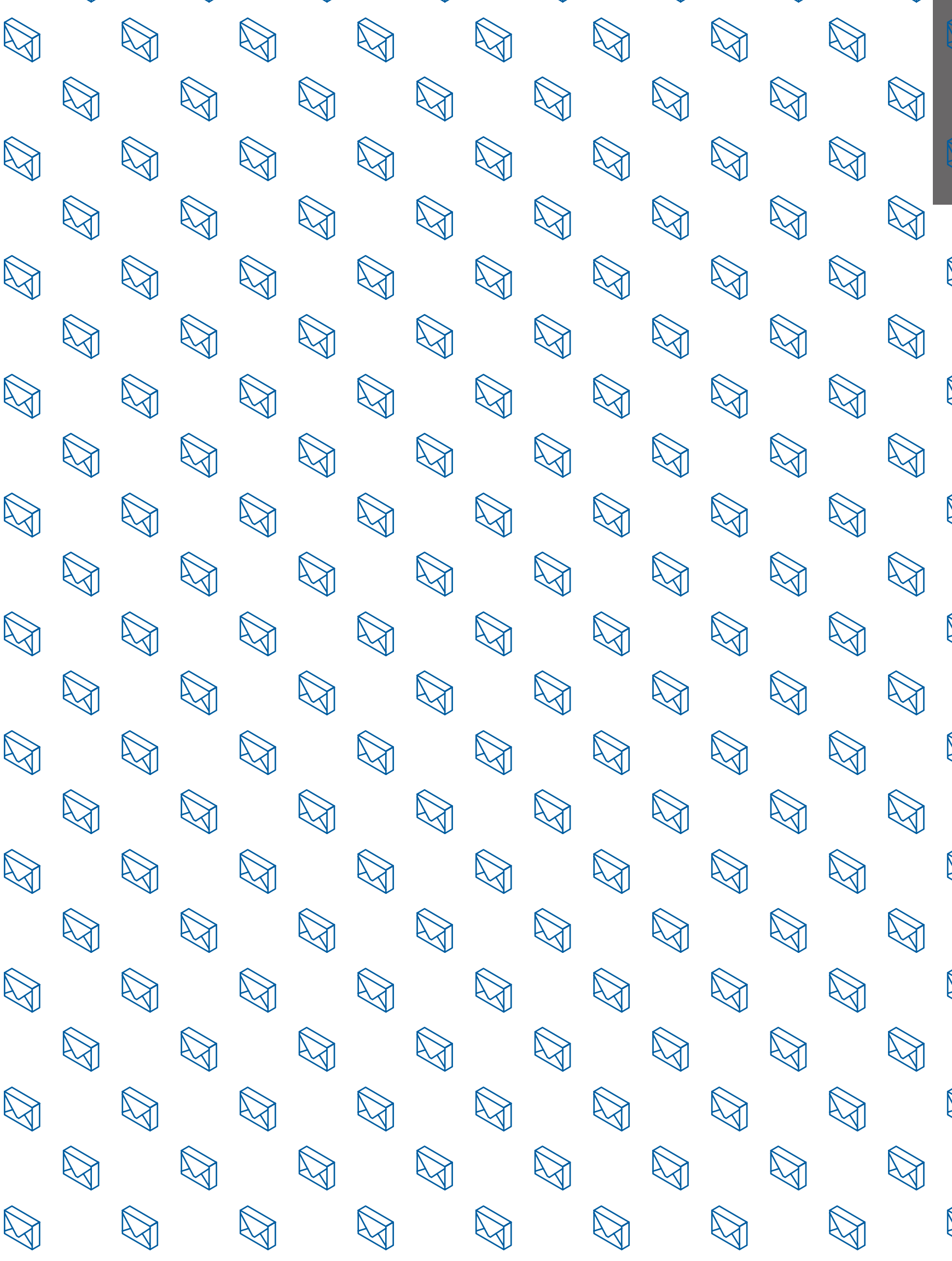
تمام مطالب آموزشی این برنامه را می‌توانید در صفحه منابع ما به آدرس اینترنتی g.co/BeInternetAwesomeEducators پیدا کنید.

آیا انجمنی آنلاین از کاربران این برنامه به منظور به اشتراک گذاشتن ایده‌ها یا کمک گرفتن از یکدیگر وجود دارد؟

بله! (و ما از این ایده بسیار استقبال می‌کنیم) ما به طور پیوسته ایده‌ها را به اشتراک می‌گذاریم و با معلمان در توییت در ارتباط

هستیم.

لطفاً برای کسب اطلاعات بیشتر در مورد Be Internet Awesome و سایر موضوعات ما را در GoogleForEdu@ دنبال کنید.



چه وقت نباید مطلبی را به اشتراک گذارد؟

دانش‌آموزان گروهی دو نفره تشکیل داده و به منظور اندیشیدن در مورد حریم خصوصی شروع به مقایسه برخی اسرار ساختگی و دروغین با یکدیگر کنند.

درباره درس: این درس به بیان این نکته می‌پردازد که حفظ حریم خصوصی افراد در اینترنت، در هر سنی که باشند، بسیار مهم است. این درس در این باره است که پس گرفتن محتوایی که در اینترنت به اشتراک می‌گذاریم، این که تعیین کنیم چه کسی محتوای اینترنتی ما را ببیند و این محتوا تا کی دیده شود، دشوار است. اگر قبل از شروع درس از دانش‌آموزان بپرسید از چه فناوری‌هایی استفاده می‌کنند و سپس به آن رسانه اجتماعی و ابزار مراجعه کنید، می‌تواند مفید باشد. اگر با چنین برنامه‌هایی آشنایی ندارید هیچ مشکلی نیست! همانطور که می‌دانید دانش‌آموزان از این که در این مورد به شما کمک کنند خوشحال خواهند شد.

اهداف درس برای دانش‌آموزان للطلاب:

- ✓ درک این نکته که چه نوع اطلاعات شخصی را باید خصوصی نگه داشت و چرا.
- ✓ یادآوری این نکته که حریم خصوصی هر فرد بایستی محترم نگه داشته شود.

بیا یاد حرف بزنیم



چرا حریم خصوصی مهم است؟

اینترنت ارتباط برقرار کردن با خانواده، دوستان و هر کس دیگر را بسیار ساده کرده است. ما پیام ارسال می‌کنیم، عکس به اشتراک می‌گذاریم، با دیگران گفتگو می‌کنیم و یا به طور زنده شروع به پخش محتوا می‌کنیم. گاه این به اشتراک گذاردن‌ها بدون در نظر گرفتن این نکته است که چه کسانی ممکن است در همان لحظه یا در آینده این محتوا را ببینند. عکس یا محتوایی که فکر می‌کنید جالب و بی‌ضرر است، ممکن است توسط افرادی که هرگز فکر نمی‌کنید آن را ببینند، چه در همان لحظه و چه در آینده، اشتباه تعبیر شود. احساسات افراد ممکن است صدمه ببیند. افرادی که شوخی شما را درک نمی‌کنند، ممکن است فکر کنند شما نیت سوئی داشته‌اید، زیرا آن‌ها شما را نمی‌شناسند. هنگامی که چیزی به اشتراک گذارده می‌شود، پس گرفتن آن دشوار است و مردم می‌توانند از آن کپی یا اسکرین‌شات گرفته و یا آن را به اشتراک گذارند. به خاطر داشته باشید:

- آنچه پست می‌کنید یا به اشتراک می‌گذارید توسط افرادی که هرگز آنها را ندیده‌اید، قابل مشاهده است.
- وقتی موضوعی را در اینترنت به اشتراک می‌گذارید ممکن است این محتوا تا ابد باقی بماند، فقط کافی است شخص دیگری از آن یک اسکرین‌شات بگیرد و آن را به اشتراک بگذارد. این کار مانند ایجاد این است که با مازیکی دائمی چیزی بنویسید که پاک کردن آن به شدت دشوار است.
- در مجموع شهرت و اعتبار شما و طرز تفکر دیگران نسبت به شما ممکن است در گروهی اطلاعات عمومی باشد که به سختی قابل پاک شدن هستند. بنابراین باید تا حد امکان بر آنچه که به اشتراک می‌گذارید کنترل داشته باشید.

به همین دلیل است که حریم خصوصی مهم است. می‌توانید با پست کردن محتوایی شخصی به طور خصوصی یا به اشتراک‌گذاری محتواهایی که از درج آنها مطمئن هستید، از حریم خصوصی خود محافظت کنید. به عبارت دیگر باید در مورد آنچه می‌گویید، پست می‌کنید و یا در اینترنت به اشتراک می‌گذارید بسیار دقت کرده و محتاطانه عمل کنید.

همچنین خوب است بدانید چه زمان نباید محتوایی را به اشتراک گذارد، در مورد پست، عکس یا نظر کسی واکنش نشان ندهید، چیزی که ممکن است درست نباشد را به اشتراک نگذارید (حتی اگر فقط یک شوخی باشد)، از به اشتراک گذاری افراطی (اشتراک‌گذاری بیش از حد) یا پست کردن اطلاعات شخصی اجتناب کنید. همگی شما توصیه «قبل از ارسال فکر کنید» را شنیده‌اید و قطعاً این توصیه بسیار خوبی است. راه احترام گذاردن به حریم خصوصی خود و دیگران این است که قبل از ارسال محتوایی در اینترنت به این موضوع بیاندیشید که به اشتراک گذاردن چه محتوایی صحیح است، چه کسی ممکن است آنچه را که به اشتراک می‌گذارید ببیند، این محتوا ممکن است چه تأثیری بر شما و دیگران داشته باشد (چه در حال حاضر و چه زمانی که همگی 16 ساله داشته باشید) و چه وقت نباید هیچ محتوایی را به اشتراک گذاشت.

برخی پرسش‌ها برای بحث و گفتگوی بیشتر (دانش‌آموزان می‌توانند این پرسش‌ها را برای گفتگوی بیشتر در منزل نیز مطرح کنند):

- چرا هرگز نباید نام کامل، آدرس، شماره تلفن و سایر اطلاعات شخصی خود را در اینترنت به اشتراک بگذاریم؟
- چه زمان می‌توان تصویر یا فیلم شخص دیگری را به اشتراک گذاشت؟
- آیا ارسال اطلاعات محرمانه یا خصوصی به دیگران کار درستی است؟ چرا بله و چرا خیر؟ آیا فکر می‌کنید این کار یک شوخی است؟
- اگر شخصی که برایتان مهم است، مطلبی خصوصی به اشتراک بگذارد که باعث شود احساس کنید ممکن است برای فرد مذکور خطری در پی داشته باشد، چه می‌کنید؟ آیا شما هم آن محتوا را به اشتراک می‌گذارید؟ آیا باید به فرد مذکور بگویید که نگران وی هستید؟ آیا باید به فرد مذکور بگویید تصمیم دارید این موضوع را به گوش بزرگسالی که به وی اعتماد دارید، برسانید؟

فعالیت



1. یک راز بسازید.

مطمئن شوید که این یک راز دروغین است نه یک راز واقعی.

2. آن راز را به شریک خود بگویید.

- خوب، راز خود را ساختید؟ حالا بیایید دو تا دوتا گروه تشکیل دهیم و راز خود را با شریک خود در میان بگذاریم و در مورد این سه پرسش با یکدیگر گفتگو کنیم:
- آیا این راز را با کسی در میان می‌گذارید؟
 - راز خود را با چه کسی در میان می‌گذارید و چرا؟
 - اگر راز شما را بدون اجازه به دیگران بگویند چه احساسی خواهید داشت؟

3. به کلاس بگویید.

در نهایت هر دانش‌آموز راز دروغین خود و احساس خود را در مورد به اشتراک گذاشتن آن برای تمام کلاس بازگو می‌کند. کل کلاس می‌تواند در مورد پاسخ‌های خود به سؤالات فوق با یکدیگر گفتگو کنند.

نکته

اسرار و رازها اطلاعاتی شخصی هستند که باید از به اشتراک گذاردن آنها در اینترنت خودداری کرده و آنها را فقط با خانواده یا دوستان قابل اعتماد خود به اشتراک گذاشت. وقتی رازی را به اشتراک گذاشتید، دیگر بر این که این راز در اختیار چه کسانی قرار خواهد گرفت کنترلی نخواهید داشت. به همین دلیل است که می‌گوییم قبل از ارسال مطلبی در اینترنت باید به خوبی فکر کرد (و این حرف بسیار درست است!). دیگر اطلاعاتی که هرگز نباید به در اینترنت به اشتراک گذاشت شامل موارد زیر هستند:

- آدرس منزل و شماره تلفن خود
- پست الکترونیکی خود
- گذرواژه‌های خود
- نام کامل خود
- نمرات و تکالیف مدرسه خود

با احتیاط به اشتراک بگذارید: درس 2 خصوصی نگه داشتن آن

چهار سناریوی نوشته شده در کلاس بررسی شده و در مورد این که بهترین راه برای حفظ حریم خصوصی در هر یک از این سناریوها چه است، بحث می‌شود.

اهداف درس برای دانش‌آموزان لطلاب:



- ✓ تجزیه و تحلیل دیدگاه‌های افراد مختلف در مورد نگرانی‌های مربوط به حریم خصوصی.
- ✓ درک این نکته که چرا سناریوهای مختلف از سطوح مختلف حریم خصوصی برخوردارند.

بباید حرف بزنیم



سناریوهای حفظ حریم خصوصی: چه باید انجام داد؟

برای کسب اطلاعات بیشتر به سناریوهای زیر نگاهی بیندازید.

فعالیت



وسایل مورد نیاز:

- طرح کلی معلم: «خصوصی نگه داشتن»

سناریوها:

پنج سناریو را بررسی می‌کنیم و در مورد این که هر کدام از این سناریوها چگونه می‌توانند راه حل‌های متفاوتی برای حفظ حریم خصوصی داشته باشند صحبت می‌کنیم. کلاس به چهار گروه تقسیم شده و هر یک از سناریوها را مورد بحث و گفتگو قرار می‌دهیم و سپس به بحث کلاسی در مورد یافته‌هایمان خواهیم پرداخت.

- سناریوی 1:** شخصی به «دانش‌آموز آ» گفته است که باید هر از چند گاهی گذرواژه‌ها و رمزهای عبور تلفن‌های خود را تغییر دهد. بنابراین «دانش‌آموز آ» تصمیم می‌گیرد رمز عبور بازی مورد علاقه خود را تغییر دهد. «دانش‌آموز ب» که بهترین دوست «دانش‌آموز آ» نیز است، دوست دارد بازی کند، اما برای ورود به بازی حساب کاربری ندارد. بنابراین «دانش‌آموز ب» از حساب کاربری «دانش‌آموز آ» استفاده می‌کند و «دانش‌آموز آ» رمز عبور جدید خود را به «دانش‌آموز ب» می‌دهد.
- آیا تغییر رمز توسط «دانش‌آموز آ» کار درستی بوده است؟
 - این که «دانش‌آموز آ» رمز عبور خود را با «دانش‌آموز ب» به اشتراک گذاشته است کار درستی بوده است؟ چرا بله و چرا خیر؟

اگر «دانش‌آموز آ» رمز عبور یکی از رسانه‌های اجتماعی خود را به اشتراک بگذارد، چه می‌شود؟ آیا پاسخ‌ها همان پاسخ‌های قبلی هستند؟ در صورتی که دانش‌آموزان دبیرستانی باشند و دوستان متفاوتی داشته باشند، آیا پاسخ‌ها باز یکی هستند؟

سناریوی 2: شخصی خاطرات خود را می‌نویسد. متوجه شده‌اید یکی از دوستان آن فرد وقتی شب در منزل دوستش بوده است آن دفترچه خاطرات را پیدا کرده است و فکر می‌کند به اشتراک گذاشتن بخش‌هایی از این خاطرات در اینترنت شومی خنده‌داری است.

- آیا کار دوست این فرد اشتباه است؟ آیا کار این فرد خنده‌دار و جالب است؟ چرا بله و چرا خیر؟
- اگر کسی همین کار را با چیزی که شما نمی‌خواهید دیگران آن را ببینند انجام دهد، چه احساسی خواهید داشت؟

سناریوی 3: شخصی در صفحهٔ رسانهٔ اجتماعی یکی از دوستانش عبارت «تعطیلاتی عالی داشته باشی» را ارسال می‌کند.

- آیا شخص به طور علنی اعلام کرده بود که دوستش به تعطیلات می‌رود؟ آیا آن شخص و خانواده‌اش می‌خواستند همه از رفتن آنها به تعطیلات باخبر شوند؟ (خوب، نه همهٔ مردم، اما مسلماً شما نباید می‌دانستید.)
- آیا راه‌های خصوصی بیشتری برای برقراری ارتباط با این پیام وجود دارد؟

سناریوی 4: دانش‌آموزی با جعل هویت شخصی دیگری یک حساب کاربری جعلی در شبکه‌های اجتماعی درست کرده است و باعث بد جلوه دادن فرد مذکور شده است و شما نیز از موضوع خبر دارید. این حساب کاربری شامل اطلاعات

شخصی فرد مذکور نیز می‌شود.

- آیا دانش‌آموزی که هویت وی جعل شده است حق دارد این موضوع را بدانند؟ آیا به او می‌گویید؟
- مشخص نیست چه کسی این حساب را ساخته است، اما شما خبر دارید چه کسی این کار را انجام داده است. آیا باید به فرد سازندهٔ این حساب کاربری جعلی بگویید حساب کاربری مذکور را پاک کند؟
- آیا باید این موضوع را به معلم یا بزرگسال مورد اعتماد خود تعریف کنید؟
- اگر کسی کاری نکند، چه اتفاقی می‌افتد؟

سناریوی 5: در منزل شما همگی به نوبت از تبلت مادران استفاده می‌کنید، بنابراین همه رمز عبور آن را بلد هستید. کل

- خانواده از یک حساب کاربری برای خرید آنلاین از وبسایتی مشخص استفاده می‌کنند. همه چیز خوب پیش می‌رفت تا این‌که روزی دوست برادرتان از تبلت مادران برای دیدن هدفون‌های شگفت‌انگیز مناسب گیمرها استفاده می‌کند. برادرتان برای آوردن خوراکی به آشپزخانه می‌رود و بعد همگی برای بازی بسکتبال بیرون می‌روید. چند روز بعد جعبه‌ای حاوی هدفون به منزل شما فرستاده می‌شود. برادرت می‌گوید که او چنین سفارشی نداده است و شما حرفش را باور می‌کنید.
- والدین شما می‌پرسند این هدفون چطور سفارش داده شده است. شما و برادرتان چه کار خواهید کرد؟
- در مورد رمز عبور چطور؟ آیا استفاده تمام افراد خانواده از گذرواژه‌های یکسان برای دستگاه‌ها و حساب‌های خانوادگی که باعث می‌شود دوستانتان نیز به این حساب‌ها و گذر واژه‌ها دسترس داشته باشند مشکل‌ساز است؟ آیا در این مورد با خانواده خود صحبت می‌کنید؟

موقعیت‌های مختلف پاسخ‌های متفاوتی را، چه به صورت آنلاین یا آفلاین، می‌طلبید. اما آنچه اهمیت بسیار دارد این است که به حریم خصوصی دیگران احترام بگذارید، حتی اگر آن‌ها انتخاب‌هایی نداشتند که خودتان انجام می‌دهید.

طرح کلی معلم: درس 2

خصوصی نگه داشتن

نکته‌ای برای آموزگاران: این بخش برای کمک به شما در جهت هدایت مباحث این درس تهیه شده است. این قسمت برای دانش‌آموزان نیست. پاسخ‌های صحیح و/یا بهترین پاسخ را روی تخته بنویسید و در مورد آن گفتگو کنید.

سناریوی 1:

آیا تغییر گذرواژه توسط «دانش‌آموز آ» کار درستی بوده است؟

بله، داشتن گذرواژه‌های مختلف برای دستگاه‌ها و سرویس‌های مختلف و تغییر این گذرواژه‌ها دست کم یک بار در سال اقدامی مناسب و صحیح در راستای حفظ حریم خصوصی است.

آیا این که «دانش‌آموز آ» رمز عبور خود را با «دانش‌آموز ب» به اشتراک گذاشته است کار درستی بوده است؟ چرا بله و چرا خیر؟

نه کار درستی نیست. ما می‌دانیم که بچه‌ها اغلب رمزهای عبور خود را با دوستان خود به اشتراک می‌گذارند و از این رو آنها باید یاد بگیرند که این کار درستی برای حفظ حریم خصوصی یا امنیت دیجیتال آنها نیست. در این قسمت می‌توانید به کشف و شناسایی دلایل خوب نبودن این کار کمک کنید. می‌توانید از دانش‌آموزان خود بپرسید «آیا می‌توانند به موقعیت‌هایی فکر کنند که دوست نداشته‌اند کسی به جز یک بزرگسال قابل اعتماد رمز عبورشان را داشته باشد؟» مثال‌ها می‌تواند شامل موارد زیر باشد:

گاهی اوقات دوستی‌ها از بین رفته و مردم از دست یکدیگر ناراحت یا عصبانی هستند. آیا دوست دارید کسی که از

دست شما عصبانی است بتواند رمز عبور شما را با دیگران به اشتراک بگذارد؟

• گر یکی از دوستان شما رمز عبور تلفن شما را داشته باشد و وارد حساب کاربری شما شود و خود را به جای شما جا بزند و صرفاً برای شوخی - درباره شخص دیگری که هر دو می‌شناسید، مطالب دروغی یا بدی بگوید، چطور؟ دیگران فکر می‌کنند شما این حرفها را زده‌اید.

اگر رمز عبور خود را با فردی که از محله یا کلاستان رفته است به اشتراک گذاشته باشید، آیا دوست دارید آن فرد

بتواند برای همیشه به حساب‌ها و اطلاعات خصوصی شما دسترسی داشته باشد؟

• اگر در حال بازی باشید و بازیکن دیگری بخواهد اجازه دهید وارد سیستم شما شده تا بتواند مانند شما بازی کند، چطور؟ اگر آن فرد دوست شما باشد باز هم اطلاعات ورود حساب کاربری خود را به او می‌دهید؟ به این فکر کنید که در بازی چه کارهایی می‌توانید انجام دهید و این که دوستان نیز می‌توانند هر چه شما انجام می‌دهید را از طریق حساب کاربری شما انجام دهد. آیا چنین چیزی درست است؟ آیا ممکن است هفته آینده یا حتی سال آینده این کار برای شما مشکلی ایجاد کند؟

اگر «دانش‌آموز آ» رمز عبور رسانه اجتماعی خود را با دوستانش به اشتراک بگذارد، چطور؟ پاسخ‌ها یکی هستند؟

وقتی آنها به سن دبیرستان برسند و دوستان متفاوتی داشته باشند نیز همین پاسخ‌ها را می‌دهند؟

• بله، همان پاسخ‌ها را می‌دهند، زیرا به اشتراک گذاشتن رمز عبور هر حساب کاربری با دوستان، حتی نزدیکترین آنها، کار درستی نیست، زیرا همانطور که گفته شد دوستی‌ها تغییر می‌کنند، گاهی اوقات دوستان شما به دوستان سابق تبدیل می‌شوند و شما نمی‌خواهید حساب یا نمایه خود را در اختیار کسی که برایتان ارزش قائل نیست، بگذارید، زیرا در این صورت آنها می‌توانند اطلاعات شما را ویرایش کنند، شما را بد جلوه دهند، یا با وانمود کردن خود به جای شما مطلبی دروغین و نامناسب را درباره شخص دیگری ارسال کرده و به اشتراک بگذارند.

سناریوی 2:

آیا این کار دوستان که اطلاعات را در اینترنت به اشتراک گذاشته است اشتباه بوده است؟ آیا چنین کاری جالب و

خنده‌دار است؟ چرا بله و چرا خیر؟

رخی دانش‌آموزان فکر می‌کنند اگر مطلبی که به اشتراک می‌گذارند خنده‌دار باشد، کار جالبی انجام داده‌اند، از این رو بهتر است کمی دقت کنید و این سوال را از آنها بپرسید:

اگر کسی این کار را با چیزی انجام دهد که شما نمی‌خواهید دیگران ببینند، چه احساسی خواهید داشت؟

سناریوی 3:

آیا یکی از دوستان شما تا به حال به طور علنی اعلام کرده است که به تعطیلات می‌رود؟

برای بحث بیشتر در این مورد فرض کنید پاسخ مثبت است، سپس از کلاس پرسید:

آیا آنها می‌خواستند همه مردم از این موضوع آگاه شوند؟ آنها به تعطیلات باخبر شوند؟

(خوب، نه همه مردم، اما مسلماً شما نباید می‌دانستید.)

• نه، (احتمالاً)

• چرا نه؟

برخی از پاسخ‌های خوب می‌تواند شامل موارد زیر باشد: ممکن است خانواده آنها بخواهند محل سکونتشان محرمانه باقی بماند و یا ممکن است نگران امنیت منزل خود؛ وقتی کسی آنجا نیست، شوند.

آیا راه‌های خصوصی بیشتری برای ارسال چنین پیامی وجود دارد؟

• آنها احتمالاً به چند پاسخ خوب خواهند رسید، به عنوان مثال ارسال پیام به صورت خصوصی، پیامک، تماس تلفنی با آنها و غیره.

سناریوی 4:

آیا دانش‌آموزی که هویت او جعل شده است حق دارد این موضوع را بداند؟ آیا به او خبر می‌دهید؟

شما پاسخ بخش اول این سوال را خواهید داشت، اما خوب است پاسخ دانش‌آموزان را هم بشنوید و در مورد آنها بحث کنید، این که آیا آنها به قربانی خبر می‌دهند و چه چیزی به وی می‌گویند.

مشخص نیست چه کسی این حساب جعلی را ساخته است، اما شما می‌دانید چه کسی این کار را انجام داده است.

آیا باید به شخص مذکور بگویید آن حساب را ببندد؟

• بسیاری از افراد از رویارویی با فرد متجاوز حس بدی دارند، و البته این اشکالی ندارد. از کلاس پرسید انجام دادن این کار برای کدام یک از آنها مشکل نیست و چرا؟ ببینید آیا این پرسش باعث ایجاد مباحث کلاسی بیشتر می‌شود.

آیا باید به معلم یا بزرگسال مورد اعتماد خود این موضوع را اطلاع داد؟

• بله، اگر کسی نباشد که به متجاوز نگوید حساب را ببندد و یا حتی اگر بعد از گفتن این موضوع بازهم حساب کاربری باز بماند در این صورت باید به بزرگتر خبر داد.

به دانش‌آموزان خود کمک کنید به این درک برسند که محافظت از دیگران در برابر آسیب‌هایی مانند آبروریزی، طردشدگی اجتماعی، آزار و اذیت و قلدری مهم است. این کار «خبرچینی» محسوب نمی‌شود. هدف همانا محافظت از دیگران است و نه به دردسر انداختن آنها.

اگر کسی این کار را نکند چه اتفاقی ممکن است رخ دهد؟

• چرخه آسیب رساندن به دیگران متوقف نخواهد شد.

• این یک نقطه آغازین مناسب برای گفتگوی کلاسی در مورد مراقبت از دیگران و علل اهمیت آن است. اطلاعات بیشتر در بخش «در اینترنتن مهربان باشید» در دسترس است.

سناریوی 5:

پدر و مادرتان نمی‌دانند این هدفون چگونه سفارش داده شده است. شما و برادرتان چه می‌کنید؟

• دانش‌آموزان ممکن است به طور غیرارادی بر روی آنچه درست است و یا نیست تمرکز کرده و به طور مثال اگر این کار درست باشد گفتگویی کوتاه در مورد آن داشته باشند تا ببینند آیا نظر آنها با جمع یکی است یا خیر!

در مورد بخش گذرواژه چطور؟ در مورد خطرات استفاده تمام افراد خانواده از رمزهای عبور یکسان برای دستگاه‌ها و

حساب‌های کاربری خانواده صحبت کنید.

بسیاری از خانواده‌ها چنین کاری انجام می‌دهند. ببینید آیا می‌توانید دانش‌آموزان را به اندیشیدن با صدای بلند در مورد (1) محافظت از رمزهای عبور خانواده به هنگام آمدن دوستان به منزل، (2) این که چرا نباید رمزهای عبور خانواده را با دوستان و دیگر افراد خارج از خانواده به اشتراک گذاشت و (3) این که به جز امکان سفارش دادن توسط دوستان چه مشکلات دیگری ممکن است برای یک حساب کاربری خانوادگی رخ دهد، ترغیب نمایید.

اگر شما از «کد» طرفداران تیم پکرز اطلاعی نداشته باشید، ممکن است فکر کنید که این کلاه پنبه‌ری بخشی از لباس هالووین یا فقط یک کار عجیب است. حتی ممکن است بخواهید در مورد عجیب بودن چنین کاری اظهار نظر کنید. این کار ممکن است طرفداران تیم پکرز را عصبانی کند. از نظر آنها، نظر شما بی‌ادبانه است و ممکن است آنها نیز بخواهند پاسخ بدی به نظر شما بدهند. این کار شما را عصبانی می‌کند، بنابراین ما با انبوهی از نظرات منفی و احساسات جریحه دار شده مواجه خواهیم شد.

بنابراین چگونه می‌توان مطمئن شد که دیگران منظورمان را از مطلبی که در اینترنت به اشتراک گذاشته‌ایم، متوجه خواهند شد؟ یکی از راه‌ها این است که خودمان را خالق رسانه ببینیم، و نه فقط ارتباط‌دهنده یا پخش‌کننده آن. هر بار که یک نمایه آنلاین ایجاد می‌کنیم، به کسی پیام می‌دهیم، با دیگران صحبت می‌کنیم و یا تصویری را به اشتراک می‌گذاریم، در حال ساخت رسانه هستیم. مانند دیگر سازندگان رسانه‌های خوب ما نیز باید در مورد رسانه‌ای که می‌سازیم و به اشتراک می‌گذاریم دقت کرده و قبل از به اشتراک گذاردن آن کمی درنگ کرده و از خود بپرسیم: «کسی که با من متفاوت است پیام من را چگونه تفسیر خواهد کرد؟»

فعالیت:



وسایل مورد نیاز:

- پخش شود: «تی‌شرت سفید، بدون هیچ طرحی» (یک عدد برای هر دانش‌آموز)
- پخش شود: «تصاویر ایموجی» (روی تخته کلاس نصب شده و یا برای دانش‌آموزان ارسال شود به نحوی که همه بتوانند آنها را ببینند)
- ماژیک، مداد رنگی، یا مداد طراحی
- نوار چسب (یا راهی برای نصب کردن ایموجی نقاشی شده بر روی تی‌شرت به هنگام راه رفتن دانش‌آموز)

1. خودتان را با استفاده از ایموجی‌ها معرفی کنید.

برای اینکه بتوانیم همچون یک خالق زبردست رسانه فکر کنیم، باید تی‌شرت‌ها را طراحی کنیم. با استفاده از تی‌شرت‌های ساده و تنها با استفاده از ایموجی تصویری از خود بکشید. می‌توانید از یک، دو یا سه ایموجی استفاده کنید، اما نه بیشتر. می‌توانید ایموجی‌ها را طبق تصاویر داده شده بکشید و یا خود ایموجی جدیدی ابداع کنید.

2. نشان دهید و بگویید.

گروه‌های دوتایی تشکیل دهید و سعی کنید حدس بزنید ایموجی کشیده شده بر روی تی‌شرت دوستان چه مفهومی دارد. آیا حدس شما درست است یا باید به یکدیگر توضیح دهید ایموجی‌های انتخابی‌تان چه معنایی دارد؟

3. درباره یکدیگر بیاموزید.

«تی‌شرت‌ها» را در اطراف کلاس نصب کرده تا همه بتوانند آن‌ها را ببینند. آیا می‌توانید دقیقاً هر پیراهن را با صاحب آن مطابقت دهید؟

4. گفتگوی کلاسی راه بیان‌ازید:

• چه چیزی تطبیق دادن تی‌شرت‌ها را با هم‌کلاسی‌ها سخت یا آسان کرده است؟ در مورد نمادهای روی تی‌شرت‌ها که به راحتی با یکدیگر مطابقت داده می‌شدند، متوجه چه چیز شدید؟ آیا برخی ایموجی‌ها توسط افراد زیادی استفاده شده است؟ آیا برخی از آنها فقط توسط یک نفر استفاده شده است؟

آیا همه دانش‌آموزان در مورد معنای ایموجی‌ها با یکدیگر توافق داشتند؟ چگونه «زمینه» می‌تواند معنای ایموجی را تغییر دهد؟ به ایموجی که دو انگشت دستش را بالا برده است نگاه کنید. از کجا می‌توان فهمید که این ایموجی به معنای صلح، پیروزی یا عدد 2 است؟ ایموجی آتش چطور؟ آیا به معنای خطر/موضعیت اضطراری است؟ به معنی محبوب بودن یا موفقیت است؟ (خیلی خوش تپیی، رفیق!) آیا بسته به جایی که ایموجی به کار برده می‌شود، معنی آن تغییر خواهد کرد (ایموجی‌های لبخند با دهان باز زیر تکالیف مدرسه می‌تواند به این معنی باشد که معلم شما فکر می‌کند تکلیف خود را خوب انجام داده‌اید اما در متنی از طرف یک دوست ممکن است به این معنی باشد که او خوشحال است یا شوخی می‌کند)؟ آیا بسته به ایموجی‌های دیگر در کنار این ایموجی معنی تغییر می‌کند؟

نکته

ه عنوان خالق رسانه، قبل از ارسال پیام یا عکسی در اینترنت خوب است کمی درنگ کرده و از خود بپرسید: «کسی که با من متفاوت است چگونه ممکن است پیام مرا تفسیر کند؟ آیا اطمینان دارم که آنها متوجه منظورم خواهند شد؟» آیا ممکن است این افراد برداشتی اشتباهی داشته باشند؟ و همچنین قبل از گذاشتن پستی یا ارائه نظری در اینترنت باید از خود بپرسیم: «آیا مطمئن هستم که منظور آنها را درست فهمیده‌ام؟ از کجا می‌توانم بفهمم؟»

منظورم این نبود!

در مورد درس: دانش‌آموزان با استفاده از برخی ایموجی‌ها، تی‌شرت‌هایی برای معرفی خود تهیه می‌کنند. در طی این فرآیند یاد می‌گیرند افراد مختلف ممکن است یک پیام را به شکلی متفاوت تفسیر کنند.

پیشینه سواد رسانه‌ای برای معلمان: وقتی ما تی‌شرت‌هایی با تصاویری از نماد تجاری شرکت‌ها، تیم‌های ورزشی، مدارس، موسیقی‌دانان، سیاستمداران و غیره می‌پوشیم، در واقع در حال تبلیغ کردن آنها هستیم. این فعالیت نشان می‌دهد که یک تی‌شرت می‌تواند همزمان ارتباطی مستقیم و رسانه‌ای ایجاد کرده و به دانش‌آموزان کمک می‌کند به درک این نکته برسند که صفحه نمایش تنها مکانی نیست که می‌توان رسانه‌ها را در آن یافت.

اهداف درس برای دانش‌آموزان



- ✓ **دانش‌آموزان** اهمیت طرح این پرسش را می‌آموزند: آیا ممکن است تعبیر دیگران از پیام من با آنچه منظورم بوده است، متفاوت باشد؟
- ✓ **افزایش** آگاهی نسبت به بسیاری از نشانه‌های بصری که مردم برای برقراری ارتباط استفاده می‌کنند.
- ✓ **درمی‌یابند** اشتراک گذاری مطلبی به طور آنلاین به اندازه اشتراک گذاری آن مطلب بر روی یک تی‌شرت باعث ایجاد رسانه می‌شود
- ✓ **معنی** «زمینه» و «بازنمایی» را می‌آموزند.

بیابید حرف بزیم



بیابید حرف بزیم.

آیا تا به حال کسی در مورد موضوعی که گفته‌اید، کاری که انجام داده‌اید، یا مطلبی که نوشته یا به اشتراک گذاشته‌اید دچار سوءتعبیر شده است؟

آیا آنها عصبانی یا غمگین شدند و شما مجبور شدید به آنها توضیح دهید منظور شما آن چه فکر می‌کنند، نبوده است.

گاهی اوقات وقتی در حال برقراری ارتباط هستیم، می‌دانیم منظورمان چیست، اما افرادی که با آنها ارتباط برقرار می‌کنیم متوجه این موضوع نیستند، بویژه اگر در محیط مشابه‌ای قرار نداشته باشیم. علت این است که تجربیات افراد بر نحوه تفسیر آنها از چیزهایی مانند تصاویر و کلمات تأثیر می‌گذارد.

پیام‌های بسیاری وجود دارد که ما حتی بدون این که معنی آنها را بدانیم با دیگران به اشتراک می‌گذاریم و همین امر منجر به سردرگمی و سوءتعبیر بیشتر می‌شود. ما با استفاده از نشانه‌هایی همچون لباس، مدل مو و حتی نحوه راه رفتن و حرکات بدنمان خود را به مردم معرفی کرده و یا دیگران را قضاوت می‌کنیم. چنین چیزی «بازنمایی» نامیده می‌شود، یعنی بیان چیزی در مورد موضوعی، شخصی یا گروهی با استفاده از تصاویر، نمادها، سبک‌ها و کلمات.

مثالی در اینجا آورده شده است: اگر آنلاین باشید و تصویر شخصی را ببینید که پیراهنی ورزشی با نماد یک تیم مشخص را پوشیده است، ممکن است فکر کنید که آن فرد از طرفداران آن تیم است، که در این صورت به احتمال زیاد حق با شماست. این به این دلیل است که اکثر ما طراحی پیراهن‌های ورزشی را می‌شناسیم و می‌دانیم که این یک «کد» ورزشی است. بنابراین حتی اگر مطمئن نباشیم کدام تیم بازنمایی شده است، می‌دانیم که احتمالاً یک تیم ورزشی است.

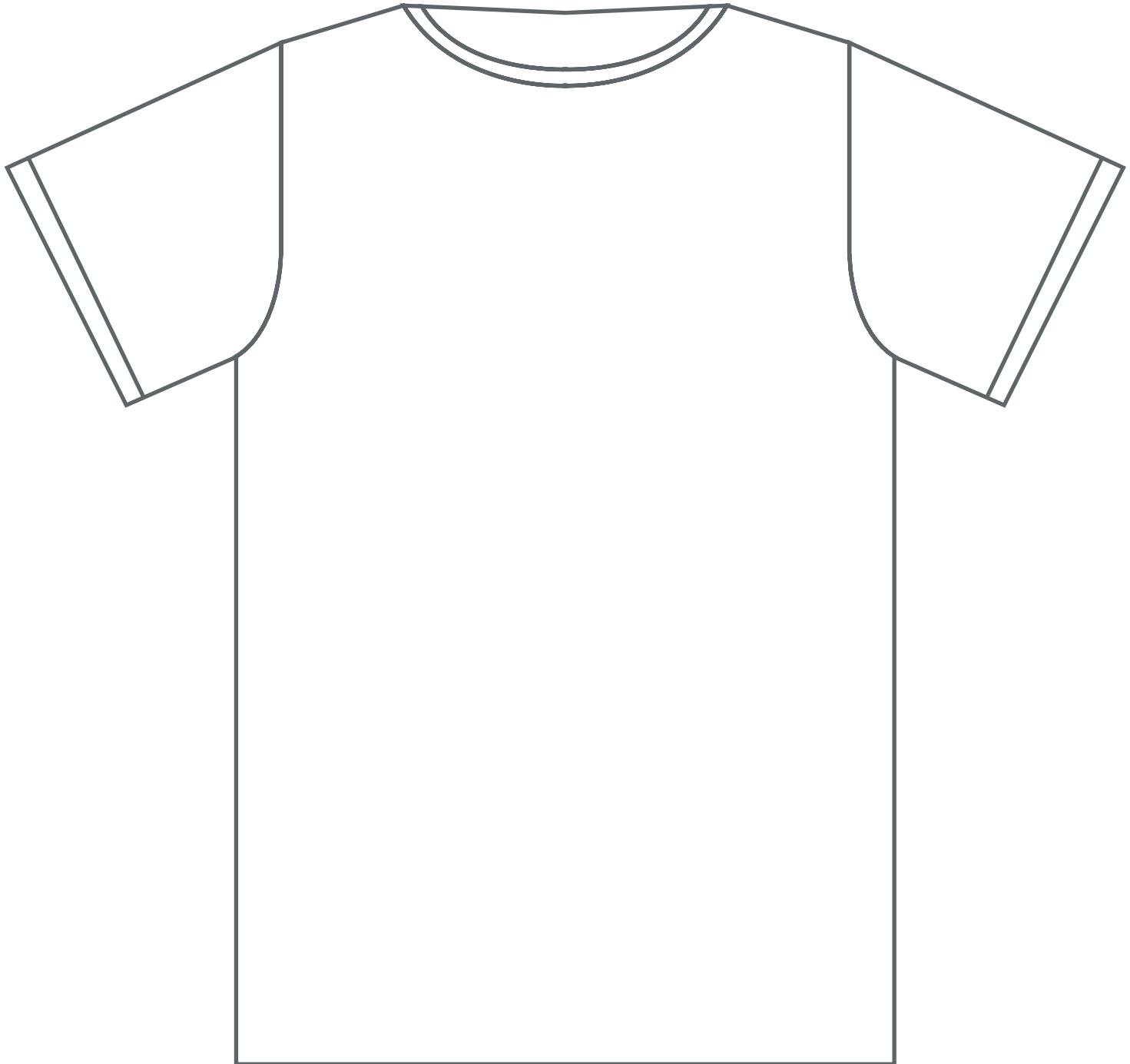
حال اگر عکس شخصی را دیدید که روی سرش یک کلاه پنی‌ری گذاشته است، چه؟ در مورد آن شخص چه فکر می‌کنید؟ اگر در «ویسکانسین» زندگی می‌کنید یا جزو طرفداران فوتبال آمریکایی باشید، می‌دانید که معنای عبارت «سر پنی‌ری» نام مستعار طرفداران فوتبال «گرین بی پکرز» است. شخص در تصویر از کلاه پنی‌ری برای نشان دادن حمایت خود از تیم مورد علاقه خود استفاده کرده است.

اگر شما از «کد» طرفداران تیم پکرز اطلاعی نداشته باشید، ممکن است فکر کنید که این کلاه پنی‌ری بخشی از لباس هالووین یا فقط یک کار عجیب است. حتی ممکن است بخواهید در مورد عجیب بودن چنین کاری اظهار نظر کنید. این کار ممکن است طرفداران تیم پکرز را عصبانی کند. از نظر آنها، نظر شما بی‌ادبانه است و ممکن است آنها نیز بخواهند پاسخ بدی به نظر شما بدهند. این کار شما را عصبانی می‌کند، بنابراین ما با انبوهی از نظرات منفی و احساسات جریحه دار شده مواجه خواهیم شد.

توزیع شود: درس 3
نمونه ایموجی‌ها



توزیع شود: درس 3
تی شرت سفید



با احتیاط به اشتراک بگذارید: درس 4 کادر بندی کنید.

پیشینه سواد رسانه‌ای معلمان: رسانه‌ها توسط افرادی ساخته می‌شوند که دست به انتخاب می‌زنند. اساسی‌ترین انتخاب چیزی است که درج شده و حذف می‌شود. این درس به دانش‌آموزان کمک خواهد کرد تا در حین تصمیم‌گیری در این خصوص که چه محتوایی را در اینترنت به اشتراک بگذارند، خود را به عنوان یک خالق رسانه در نظر بگیرند.

اهداف درس برای دانش‌آموزان لطلاب:



- ✓ **تجسم** خود به عنوان خالق رسانه.
- ✓ **درک** این موضوع که رسانه‌سازان در مورد این که چه چیز را نشان دهند و چه چیزی را خارج از کادر نگه دارند، دست به انتخاب می‌زنند.
- ✓ **از مفهوم** کادر بندی برای درک تفاوت بین آنچه که باید قابل مشاهده و عمومی باشد و آنچه که باید امن یا نامشهود نگه داشته شود، استفاده می‌کنند.

بیا یاد حرف بزنیم



سازندگان رسانه‌های بصری میزان اطلاعاتی که خواهان به اشتراک گذاردن آنها هستند را با کادر بندی کنترل می‌کنند. آن‌ها تصمیم می‌گیرند چه چیز درون کادر باشد (**آنچه می‌توانیم ببینیم**)، و چه چیزی خارج از کادر باقی بماند (**آنچه نامشهود است**).

فعالیت



فعالیت به صورت کلاسی اجرا شود و بعد در مورد آن گفتگو کنید:

1. کادر بندی

تمامی بخش‌های یک رسانه محصول انتخاب‌های سازندگان رسانه است. یک انتخاب مهم این است که چه چیز را درج و چه چیز را حذف کنیم. وقتی عکس یا فیلمی می‌گیریم، دنیای خارج از دنیای داخل تصویر یا فیلم از طریق کادر جدا می‌شود. برای این که با نحوه کارکرد این بخش آشنا شوید، برگه یادداشتی بردارید و از وسط آن مستطیلی در آورده و به این طریق کادر خود را تهیه کنید.

کادر را از خود دور نگه دارید، آن را به آرامی به سمت صورت خود نزدیک کرده و مجدداً به عقب برگردانید (می‌توانید این کار را با عملکرد زوم در دوربین امتحان کنید). در مورد آنچه در داخل کادر می‌بینید متوجه چه می‌شوید؟ اگر کادر را به سمت دیگر حرکت دهید، چطور؟ آیا می‌توانید کادر را طوری نگهدارید که برخی از همکلاسی‌های خود را ببینید و برخی دیگر را نه، یا برخی از چیزهای روی دیوار را ببینید اما برخی دیگر را نبینید؟

وقتی کادر را کنترل می‌کنید، در واقع شما سازنده رسانه هستید. شما از این قدرت برخوردارید که تصمیم بگیرید چه چیزی را در کادر خود بگنجانید یا کنار بگذارید. آنچه خارج از کادر شما است همچنان در زندگی واقعی وجود دارد، اما افرادی که رسانه‌هایی را که شما ساخته‌اید را مشاهده می‌کنند، هرگز نمی‌توانند آن بخش‌ها را ببینند.

2. آن را نگه دارید یا کنار بگذارید؟

جزوه را بردارید و به تصویر 1A نگاه کنید. فکر می‌کنید به چه چیزی نگاه می‌کنید و چگونه متوجه این موضوع شدید؟ حال به تصویر 1B نگاه کنید. اطلاعات اضافه شده چگونه به شما کمک خواهند کرد نسبت به آنچه به آن نگاه می‌کنید چشم‌انداز بهتری داشته باشید؟

وسایل مورد نیاز:

- برگه یادداشت و قیچی (یک مجموعه برای هر دانش‌آموز)
- جزوه: «چه چیز در کادر است؟» یا صفحه نمایش یا تخته هوشمند با تصاویر نمایش داده شده

این کار را با تصویر 2A نیز انجام دهید. به نظر شما این تصویر سایه چه چیزی است؟ دلیل شما چیست؟ تصویر 2B اطلاعات بیشتری به شما می‌دهد. آیا حدس شما درست بود؟

3. اطلاعات بیش از حد (TMI)

اطلاعات اضافی همیشه هم پسندیده نیستند. گاهی اوقات اطلاعات بیشتر باعث حواس پرتی ما شده و توانایی ما را در لذت بردن یا درک تصویر مندرج در کادر کوچکتر از بین می‌برد. به مثال شماره 3 در جزوه نگاهی بیندازید.

گاهی اوقات مشاهده روند ساخت برخی چیزها لذت بخش است. اما اگر هر بار که یک فیلم، یک برنامه تلویزیونی یا ویدیویی را تماشا می‌کنید، فقط یک کادر کوچک را ندیده و تمام دوربین‌ها، میکروفون‌ها، عوامل و کارکنان را می‌دیدید چطور؟ آیا فکر می‌کنید از داستان به همان اندازه لذت می‌بردید؟

4. خود تصمیم بگیرید.

هر بار که موضوعی را به طور آنلاین به اشتراک می‌گذارید، در حال ساخت رسانه هستید. و مانند تهیه‌کنندگان فیلم، ویدیو یا برنامه تلویزیونی، می‌توانید تصمیم بگیرید که مردم چه چیزی را ببینند، یعنی چه چیز درون کادر باشد و چه چیز خارج از دید و خارج از کادر قرار بگیرد.

به عنوان یک سازنده رسانه، شما یک «کادر» در اطراف آنچه به صورت آنلاین به اشتراک می‌گذارید قرار می‌دهید تا دیگران فقط آنچه را که شما می‌خواهید ببینند.

نکته

با احتیاط به اشتراک بگذارید: درس 4
کادر بندی کنید.



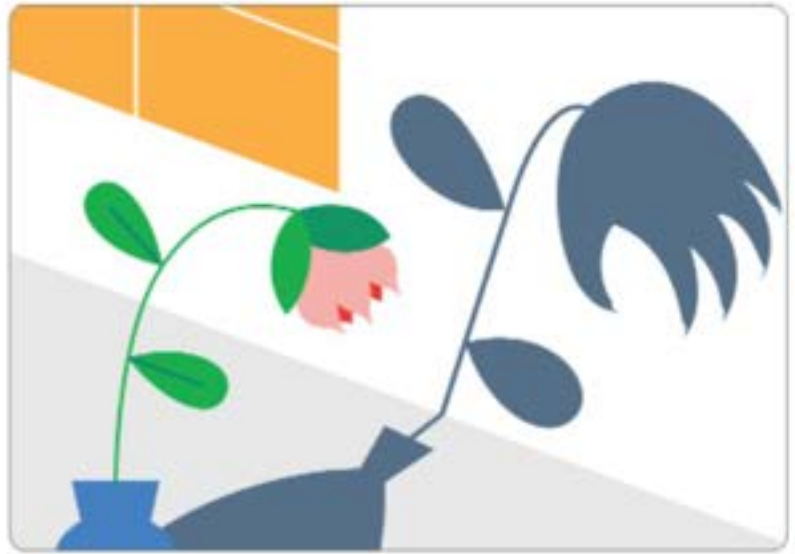
1A



1B



2A



2B



3A



3B

با احتیاط به اشتراک بگذارید: درس 5 اصلاً این شخص کیست؟

این درس به ذکر نمونه‌هایی از «ردپای دیجیتالی» می‌پردازد. دانش‌آموزان مجموعه‌ای از اطلاعات شخصی درباره یک شخصیت ساختگی را مطالعه می‌کنند- بخشی از ردپای شخصیتی فرد- و تلاش می‌کنند در مورد این فرد دست به استنباط بزنند.

اهداف درس برای دانش‌آموزان



- ✓ شناسایی راه‌هایی که می‌توان از طریق اینترنت اطلاعاتی در مورد دیگران به دست آورد.
- ✓ به این نکته دست یابند که چگونه ممکن است فردی را تنها از طریق مطالبی که به صورت آنلاین به اشتراک می‌گذارد، یعنی ردپای دیجیتالی وی، قضاوت کرد.
- ✓ دقت اطلاعات را مشخص کرده و تفاوت بین فرضیه، نظریه و واقعیت را درک کنند.

بیابید حرف بزیم

آنچه را که (فکر می‌کنیم) می‌دانیم، چگونه فهمیده‌ایم؟

- بسیاری از اطلاعات شخصی را می‌توان در اینترنت یافت. برخی از این اطلاعات ممکن است باعث شوند به چیزهایی فکر کنیم یا در مورد دیگران حدس‌هایی بزیم که درست نیستند. اینها سوالاتی هستند که ما به بررسی آنها خواهیم پرداخت:
- از اطلاعات شخصی یا آنچه فردی در اینترنت به اشتراک می‌گذارد در مورد آن فرد چه می‌فهمیم؟
 - از اطلاعات شخصی دیگران می‌توان چه چیز را در مورد آنها حدس زد، حتی اگر مطمئن نباشیم؟
 - آیا می‌دانیم این اطلاعات در وهله اول چگونه جمع‌آوری شده‌اند؟ چگونه می‌توانیم منبع را شناسایی کنیم؟

فعالیت



وسایل مورد نیاز:

- کاربرگ: « اصلاً این شخص کیست؟ » (یکی برای هر دانش‌آموز)

اصلاحات احتمالی برای کلاس‌های 2-3: اگر فکر می‌کنید دانش‌آموزان کلاس دوم یا سوم آماده هستند در مورد «ردپای دیجیتالی» در رسانه صحبت کنند، از استراتژی «من انجام می‌دهم، ما انجام می‌دهیم، شما انجام می‌دهید» استفاده کنید (به این صورت که مثال اول کاربرگ را مدل‌سازی کنید، مثال دوم را در کلاس کامل کنید و سپس آن‌ها را در اختیار تک‌تک دانش‌آموزان قرار داده و در مورد آن‌ها بحث کنید).

1. به مطالعه و بررسی فردی بپردازید.

از کلاس بخواهید اطلاعات ارائه شده درباره کریستی، تایلر، کانر یا شخصیت تخیلی که خود خلق کرده‌اند را مطالعه کنند.

2. توصیفی در این مورد بنویسید.

کلاس را گروه‌بندی کنید و به هر گروه یک شخصیت بدهید. هر گروه شرح مختصری در مورد شخص مذکور تهیه کرده و به این سؤال پاسخ دهد: «به نظر شما این شخص کیست؟»

3. توضیحات را بخوانید.

هر گروه توصیف شخصیت مورد نظر را می‌خواند.

4. حقیقت را آشکار کنید.

خوب، حقیقت در مورد شخصیت‌ها اینجا است. بیابید این حقایق را با تفکرات خود در مورد این افراد که از طریق اطلاعاتی که آنها به اشتراک گذاره بودند به دست آورده بودید، مقایسه کنید.

- کریستی سال آخر دبیرستان است. او سال آینده به دانشگاه می‌رود و امیدوار است بتواند در رشته مهندسی شیمی تحصیل کند و در نهایت قصد دارد شرکت خود را راه‌اندازی کند. او بیشتر به خانواده، کار داوطلبانه، فرهنگ پاپ و مد اهمیت می‌دهد.
- تایلر بازیکن اصلی تیم بیسبال دبیرستانش است. او 15 سال دارد و در فیلادلفیا زندگی می‌کند. او یک خواهر 8 ساله دارد. او بیشتر به این موارد اهمیت می‌دهد: بیسبال، مطالعه هنر، نواختن گیتار، معاشرت با دوستان.
- کانر 14 سال دارد. او به تازگی به تیم فوتبال پیوسته است و دو گربه دارد. طراحی او بسیار خوب است و دوست دارد آخر هفته‌ها ربات بسازد. او بیش از هر چیز به فناوری، تیم فوتبال، حیوانات و حقوق حیوانات اهمیت می‌دهد.

5. بحث کنید.

توصیف شما از شخصیت‌ها چقدر به حقیقت نزدیک بود؟ فکر می‌کنید چرا چنین توصیفی از شخصیت‌ها داشتید؟ توصیفات شما نظر است یا فرض یا حقیقت؟ دلیل آن را توضیح دهید؟ از این درس چه آموختید؟

نکته

وقتی پست‌ها، نظرات، عکس‌ها و فیلم‌های دیگران را می‌بینیم یا می‌شنویم، در مورد این افراد حدس‌هایی می‌زنیم که همیشه هم درست نیستند، بخصوص اگر این افراد را نشناسیم. دلیل این حدسیات گاهی اشتباه این است که آنچه ما به صورت آنلاین یا در یک لحظه خاص از زمان می‌بینیم، تنها بخشی از شخصیت این افراد یا چیزی که به آن اهمیت داده‌اند، است. همچنین ممکن است برخی به کاری تظاهر کرده و یا فقط احساسات سطحی یا لحظه‌ای خود را به اشتراک بگذارند. تا زمانی که شخصا این افراد را نشناسیم، نمی‌توان متوجه شد که آن‌ها واقعا که هستند یا چه احساسی دارند و حتی اگر آنها را بشناسیم، درک احساسات یا شناخت کامل افراد زمان می‌برد!

کاربرگ: درس 5

این شخص کیست؟

مجموعه‌ای از فعالیت‌های آنلاین شخصی را در ادامه می‌خوانید. بر اساس آنچه در اینجا می‌بینید، فکر می‌کنید این شخص چه ویژگی‌هایی دارد؟ بگویید این فرد ممکن است چه چیز را بیشتر دوست داشته باشد، چه چیز را دوست نداشته باشد و به چه چیز بیشتر اهمیت دهد؟

کریستی

تصاویری از رقص زیر دریا! خوب به نظر می‌رسد!

بهترین راهکار برای از بین بردن جوش صورت

برادر کوچکم، الکس، خیلی دردرس ساز است. شاید او بیگانه‌ای از یک سیاره دیگر است.

برگه جریمه به خاطر سرعت غیرمجاز

کنفرانس شیمیدانان جوان در دانشگاه تامپسون

بالاخره فیلم جدید «ماموریت‌های محرمانه» را دیدم. اوه، خدای من، فکرم را مشغول کرده است.

تایلر

بازی را برنده شدید! یک بازی دیگر تا قهرمانی باقی مانده است. باید پرتاب‌های بیشتری تمرین کرد.

از کلاس رقص مدرسه متنفرم #نرفتن

موزه فیلد، شیکاگو، ایلینویز

برای تولد 25 سالگی‌ام به سیاتل می‌روم! نمی‌توانم منتظر بمانم.

بازی با پدر در پارک پنی‌پک! عالی است!

پارک لا لونا در مرکز شهر

کانر

بازار بزرگ بارنی برگ

گل پیروزی را از دست دادیم. اوه، حداقل مساوی شدیم.

25 عکس توله سگ

جشن وستفیلد جونیور

وبسایت دوست من را بررسی کنید! من کدهای زیادی برای آن نوشتم.

بالاترین امتیاز! بللله! من عاشق این بازی هستم.

با احتیاط به اشتراک گذارده شود: درس 6

دیگران چگونه از آنلاین بودن ما با خبر می‌شوند؟

دانش‌آموزان به بررسی این نکته می‌پردازند که با توجه به مباحث درس پیش افراد مختلف مانند والدین، کارفرمایان، دوستان و پلیس شخصیت آنها را چگونه تصور کرده و چه بخش‌هایی از ردپای دیجیتالی آن‌ها حاوی اطلاعاتی در مورد آنها هستند.

اهداف درس برای دانش‌آموزان

- ✓ در تصمیم‌گیری در این خصوص که اطلاعاتی را در اینترنت به اشتراک بگذارند یا خیر، دیدگاه‌های افراد دیگر را درک کنند.
- ✓ عواقب افزایش اطلاعات شخصی خود را در نظر بگیرند: آنچه به اشتراک می‌گذارید بخشی از ردپای دیجیتالی شما خواهد بود که می‌تواند برای مدت زمانی طولانی باقی بماند.
- ✓ آغاز تفکر در این باره که منظور از گزینش محتوایی که در اینترنت به اشتراک گذارده می‌شود، چه است و چگونه این کار به ردپای دیجیتالی آنها مربوط می‌شود.



یک دیدگاه جدید

اطلاعات موجود در ردپای دیجیتالی شما می‌تواند چیزهای بیشتر یا حتی متفاوتی را در مورد شما به دیگران بگوید. ما عواقب این موضوع را بررسی خواهیم کرد.

بیا بید یکی از شخصیت‌ها را انتخاب کنیم و خود را جای وی بگذاریم و فرض کنیم نظرات او را ما ارسال کرده‌ایم. ما دیدگاه آنها را امتحان خواهیم کرد.

- به نظر شما آیا شخصیت شما می‌خواهد مردم از اطلاعات شخصی وی باخبر باشند؟ چرا بله و چرا خیر؟ شخصیت شما دوست دارد چه نوع افرادی اطلاعات شخصی شما را دانسته و چه افرادی ندانند؟
- فکر می‌کنید این اطلاعات توسط دیگران چگونه دیده می‌شود؟ به نظر شما این اطلاعات چگونه توسط دیگران استفاده می‌شود؟

بیا بید حرف بزنیم



موقعیت‌های مختلف سطوح مختلفی از حریم خصوصی را می‌طلبند. اندیشیدن به این موضوع که دیدگاه دیگران در خصوص مطالبی که در اینترنت به اشتراک می‌گذارید چه است، کلید عادت خوب حفظ حریم خصوصی در اینترنت است.

فعالیت



اصلاحات احتمالی برای کلاس‌های 2-3: اگر فکر می‌کنید دانش‌آموزان کلاس دوم یا سوم آماده هستند در مورد «ردپای دیجیتال» در رسانه صحبت کنند، از استراتژی «من انجام می‌دهم، ما انجام می‌دهیم، شما انجام می‌دهید» استفاده کنید (به این صورت که مثال اول کاربرگ را مدل‌سازی کنید، مثال دوم را در کلاس کامل کنید و سپس آن‌ها را در اختیار تک‌تک دانش‌آموزان قرار داده و در مورد آن‌ها بحث کنید).

1. دیدگاه جدیدی داشته باشید.

در کلاس چرخیده و گروه‌های کلاسی سه نفره تشکیل می‌دهیم. گروه 1 کریستی، گروه 2 تایلر و گروه 3 کانر نام دارد. سپس من (معلم) نزد هر گروه رفته و وانمود می‌کنم که یکی از افراد زیر هستم (فهرست را بخوانید). سپس گروه با توجه به اطلاعاتی که من وانمود کرده‌ام درباره شخصیت من بحث خواهد کرد.

شما نقش والدین، افسر پلیس، همسالان، دانش‌آموز دبیرستانی و از این قبیل را بازی کرده و به اطلاعات مربوط به هر یک از شخصیت‌های مندرج در کاربرگ واکنش نشان دهید (2-3 نفر یا گروه‌هایی را انتخاب کرده و از آنها بپرسید می‌خواهند کدام یک از شخصیت‌ها باشید). برای هر نقش حداکثر 2 دقیقه وقت بگذارید.

- والدین
- دوست
- پلیس
- مربی
- کارفرما
- دانش‌آموز در 10 سال آینده
- تبلیغ کننده

وسایل مورد نیاز:

- کاربرگ: «اصلاً این شخص کیست؟» (یکی برای هر دانش‌آموز)

2. گفتگوی گروهی

هرگروه به مدت 5 تا 10 دقیقه در مورد انتخاب‌های شخصیت آنها، واکنش افرادی که معلم نقش آنها را بازی کرده است و احساس آنها نسبت به دیدگاه‌های کریستی، تاپلر و کانر بحث خواهد کرد. سپس از هر گروه می‌خواهیم گفتگوها و آموزه‌های خود در مورد انتخاب حریم خصوصی در اینترنت را با کل کلاس به اشتراک بگذارند.

3. گفتگوی کلاسی

سه نکته مهم این فعالیت چه هستند؟ آیا افراد مختلفی که اطلاعات شما را به صورت آنلاین دیده‌اند، در مورد شما فرضیات درستی داشتند؟ آیا فکر می‌کنید نظرات آنها در مورد شما مثبت بوده است یا منفی؟ آیا از پاسخ‌های آنها راضی بودید؟ فکر می‌کنید این که کسی با توجه به اطلاعاتی که در اینترنت به اشتراک می‌گذارید در مورد شما نظر منفی بدهد چه عواقبی خواهد داشت؟ حال به زعم دانستن این که چه کسانی مطالب به اشتراک گذاشته شما را در اینترنت می‌بینند، چگونه اطلاعات یا محتوای متفاوتی را انتخاب خواهید کرد؟

ممکن است افراد مختلف اطلاعات یکسانی را مشاهده کنند و از آن نتایج متفاوتی بگیرند. هرگز تصور نکنید دیگران شما را همانطور که خودتان فکر می‌کنید، می‌بینند.

نکته

با احتیاط به اشتراک بگذارید: درس 7

اینترنت: کوهستان هوشیار

مرکز کوهستانی اینترنت مکانی است که در آن همه با یکدیگر نشست و برخاست داشته و سپس مسیر خود را انتخاب می‌کنند. اما شما باید در این مرکز در مورد آنچه به اشتراک می‌گذارید و با چه کسی به اشتراک می‌گذارید بسیار آگاهانه عمل کنید. اطلاعات با سرعت نور در حرکت هستند و در میان کاربران اینترنت یک نفر است که بیش از دیگران مطلب به اشتراک می‌گذارد (اشتراک‌گذارنده افراطی).

یک مرورگر وب را در رایانه رومیزی یا دستگاه تلفن همراه خود (به عنوان مثال تبلت) باز کرده و به سایت اینترنتی g.co/MindfulMountain مراجعه کنید.

موضوعات مورد بحث

یک دیدگاه جدید

اطلاعات موجود در ردیابی دیجیتالی شما می‌تواند چیزهای بیشتر یا حتی متفاوتی را در مورد شما به دیگران بگوید. ما عواقب این موضوع را بررسی خواهیم کرد.



- بیایید یکی از شخصیت‌ها را انتخاب کنیم و خود را جای وی بگذاریم و فرض کنیم نظرات او را ما ارسال کرده‌ایم. ما دیدگاه آنها را امتحان خواهیم کرد.
- به نظر شما آیا شخصیت شما می‌خواهد مردم از اطلاعات شخصی وی باخبر باشند؟ چرا بله و چرا خیر؟ شخصیت شما دوست دارد چه نوع افرادی اطلاعات شخصی شما را دانسته و چه افرادی ندانند؟
- فکر می‌کنید این اطلاعات توسط دیگران چگونه دیده می‌شود؟ به نظر شما این اطلاعات چگونه توسط دیگران استفاده می‌شود؟

موقعیت‌های مختلف سطوح مختلفی از حریم خصوصی را می‌طلبند. اندیشیدن به این موضوع که دیدگاه دیگران در خصوص مطالبی که در اینترنت به اشتراک می‌گذارید چه است، کلید عادت خوب حفظ حریم خصوصی در اینترنت است.

فعالیت



- از دانش‌آموزان بخواهید کوهستان هوشیار را بازی کرده و از پرسش‌های زیر به منظور ایجاد مباحث بیشتر در زمینه آموزش‌های خود استفاده کنند. اکثر دانش‌آموزان از بازی انفرادی بیشتری بهره را می‌برند، اما می‌توانید از آنها بخواهید در گروه‌های دو نفره نیز این بازی را انجام دهند. این کار ممکن است برای نوآموزان کم سن و سال‌تر ارزشمند باشد.
- از میان تمام مطالبی که در بازی به اشتراک گذاشتید، کدام یک را در زندگی واقعی خود بیشتر به اشتراک می‌گذارید؟ چرا؟
- در مورد وقتی که مطلبی را به طور تصادفی به اشتراک گذاشته‌اید، بگویید.
- شخصیت «اشتراک‌گذارنده افراطی» را توصیف کرده و بگویید اعمال وی چه تأثیری بر بازی دارد.
- آیا بازی کوهستان هوشیار طرز فکر شما را در مورد به اشتراک گذاشتن محتوا در اینترنت در آینده تغییر داد؟
- یکی از تغییراتی که بعد از شرکت در این درس و انجام بازی در شما ایجاد می‌شود را نام ببرید.
- یک نمونه از پیامدهای منفی احتمالی به اشتراک گذاشتن محتوا با عموم به جای دوستانتان چیست؟
- اگر به طور تصادفی موضوعی شخصی را به اشتراک گذاشتید، چه اقداماتی می‌توانید انجام دهید؟ اگر شخصی به طور تصادفی مطلبی بسیار شخصی را با شما به اشتراک بگذارد، چطور؟

وسایل مورد نیاز:

- کاربرگ: «اصلاً این شخص کیست؟» (یکی برای هر دانش‌آموز)

2. گفتگوی گروهی

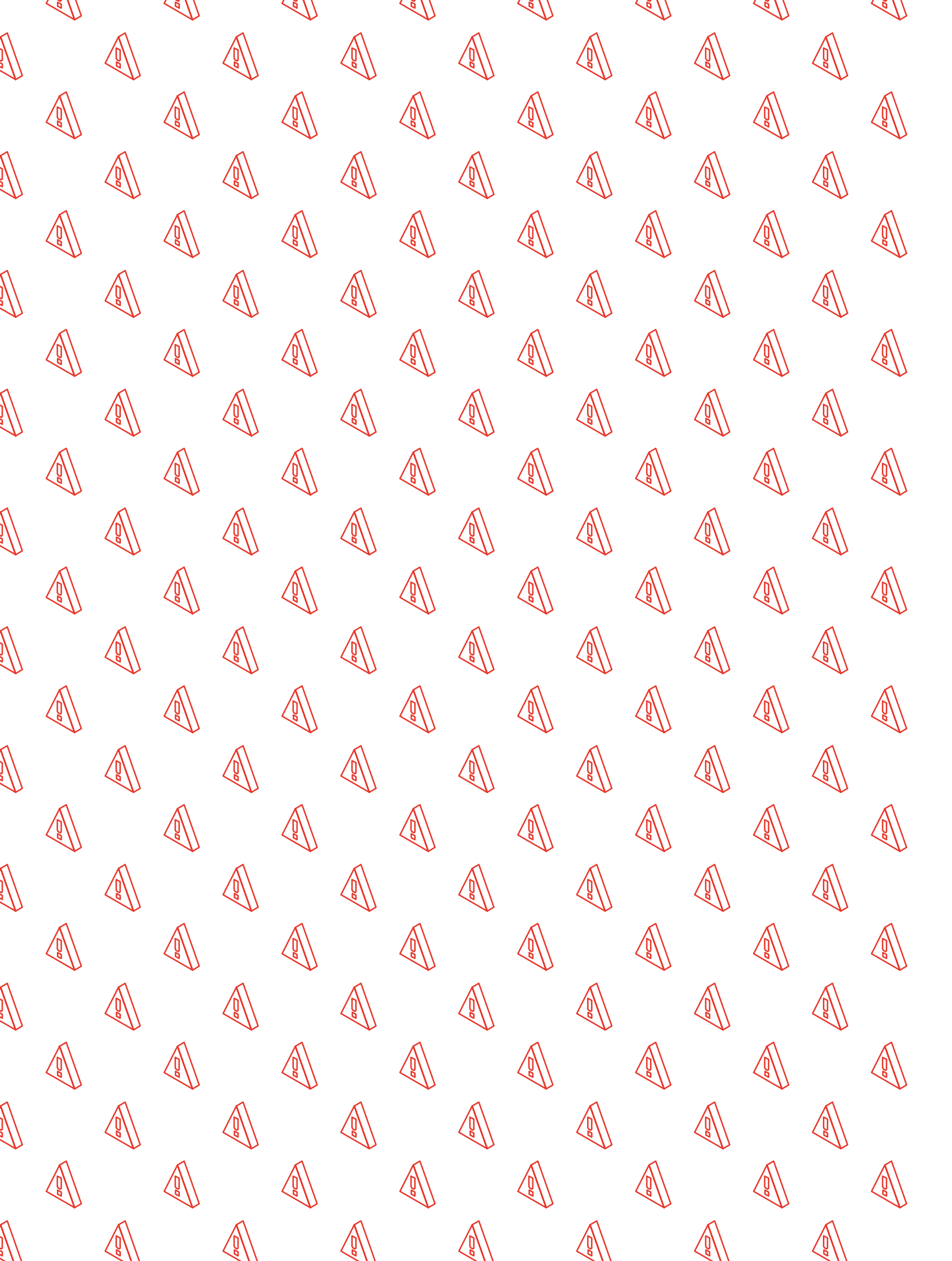
هرگروه به مدت 5 تا 10 دقیقه در مورد انتخاب‌های شخصیت آنها، واکنش افرادی که معلم نقش آنها را بازی کرده است و احساس آنها نسبت به دیدگاه‌های کریستی، تاپلر و کانر بحث خواهد کرد. سپس از هر گروه می‌خواهیم گفتگوها و آموزه‌های خود در مورد انتخاب حریم خصوصی در اینترنت را با کل کلاس به اشتراک بگذارند.

3. گفتگوی کلاسی

سه نکته مهم این فعالیت چه هستند؟ آیا افراد مختلفی که اطلاعات شما را به صورت آنلاین دیده‌اند، در مورد شما فرضیات درستی داشتند؟ آیا فکر می‌کنید نظرات آنها در مورد شما مثبت بوده است یا منفی؟ آیا از پاسخ‌های آنها راضی بودید؟ فکر می‌کنید این که کسی با توجه به اطلاعاتی که در اینترنت به اشتراک می‌گذارید در مورد شما نظر منفی بدهد چه عواقبی خواهد داشت؟ حال به زعم دانستن این که چه کسانی مطالب به اشتراک گذاشته شما را در اینترنت می‌بینند، چگونه اطلاعات یا محتوای متفاوتی را انتخاب خواهید کرد؟

ممکن است افراد مختلف اطلاعات یکسانی را مشاهده کنند و از آن نتایج متفاوتی بگیرند. هرگز تصور نکنید دیگران شما را همانطور که خودتان فکر می‌کنید، می‌بینند.

نکته



پنجره‌های پاپ‌آپ، کت‌فیشینگ و سایر کلاهبرداری‌ها

دربارهٔ درس: یک بازی که در آن دانش‌آموزان پیام‌ها و متن‌های مختلف را مطالعه کرده و در مورد این که کدام یک از پیام‌ها مشروع و قانونی بوده و کدام یک کلاهبرداری و ساختگی است تصمیم می‌گیرند.

- ✓ **تکنیک‌هایی** که برخی به منظور کلاهبرداری در محیط‌های آنلاین یا از طریق دستگاه‌های متصل شونده به اینترنت استفاده می‌کنند را فرا بگیرند.
- ✓ **شیوه‌های** پیشگیری از مورد سرقت قرار گرفتن در اینترنت را بررسی کنند.
- ✓ **در صورتی** که قربانی کلاهبرداری اینترنتی شده باشند، بایستی با بزرگتر مورد اعتمادشان در این باره صحبت کنند.
- ✓ **علائم** تلاش برای کلاهبرداری را بشناسند.
- ✓ **مراقب** باشند اطلاعات شخصی خود را با چه کسانی و چگونه به اشتراک می‌گذارند.

اهداف درس برای دانش‌آموزان للطلاب:



کلاهبرداری چیست؟

کلاهبرداری یعنی وقتی شخصی سعی می‌کند شما را فریب داده تا بتواند چیزهایی مانند گذرواژه، اطلاعات شخصی، پول یا دارایی دیجیتال شما را به سرقت ببرد. کلاهبرداران گاهی خود را به جای فرد مورد اعتماد شما جا زده و می‌توانند از طریق پنجرهٔ پاپ‌آپ، صفحهٔ وب، متن یا حتی یک برنامه جعلی در فروشگاه‌های تبلیغاتی یا یک برنامه سر راه شما قرار بگیرند. پیام‌ها و صفحات نامنی که سعی می‌کنند برای شما ارسال کنند ممکن است باعث ویروسی شدن دستگاه شما شود. برخی کلاهبرداران از فهرست مخاطبین شما به منظور هدف قرار دادن دوستان و خانوادهٔ شما به همان شیوه استفاده می‌کنند. برخی نیز سعی می‌کنند شما را فریب داده تا یک برنامهٔ ویروسی که شبیه برنامهٔ واقعی است را دانلود کنید و یا با گرفتن این که مشکلی در دستگاه شما وجود دارد شما را مجبور به دانلود کردن بدافزارها کنند.

پایید حرف بزنیم



به یاد داشته باشید: یک پیام دهنده، وبسایت یا هیچ تبلیغی نمی‌تواند تشخیص دهد دستگاه یا رایانه شما مشکلی دارد یا خیر! بنابراین اگر بگویند دستگاه یا رایانهٔ شما مشکل دارد، مطمئناً قصد کلاهبرداری از شما را دارند. همچنین به خاطر داشته باشید (ممکن است قبلاً این را شنیده باشید، اما خوب است باز بشنوید): اگر از فردی ناشناس یا حتی فردی که فکر می‌کنید ممکن است او را بشناسید پیامی دریافت کردید که بسیار جالب، هیجان‌انگیز یا بیش از حد واقعی خوب به نظر برسد، باید به آن شک کرد.

یادداشتی برای معلم:

می‌توانید از دانش‌آموزان بخواهید با بلند کردن دست خود نشان دهند آیا تا به حال در خصوص چنین کلاهبرداری‌هایی شنیده‌اند و سپس بپرسید آیا خود یا یکی از اعضای خانوادهٔ آنها تا به حال چنین پیغام‌هایی دریافت کرده است. اگر پاسخ آنها خیر باشد که جای خوشحالی دارد و اگر در آینده با چنین مواردی روبرو شوند به خوبی می‌دانند چگونه از خود، خانواده و وسایلشان محافظت کنند.

برخی کلاهبرداری‌ها بوضوح مشخص هستند، اما برخی دیگر ممکن است بسیار زیرکانه و متقاعد کننده برنامه‌ریزی شده باشند، مانند زمانی که کلاهبردار پیامی حاوی برخی اطلاعات شخصی شما را برایتان ارسال می‌کند. چنین مواردی را طعمه‌گذاری هدفمند می‌نامند و تشخیص آن ممکن است بسیار دشوار باشد، زیرا استفاده از اطلاعات شخصی شما این تصور را ایجاد می‌کند که فرد فرستنده شما را می‌شناسد. کلاهبرداری دیگری که احتمالاً نام آن را شنیده باشید جعل هویت در فضای مجازی یا همان کت‌فیشینگ است، یعنی زمانی که شخصی صفحه یا نمایه‌ای جعلی ایجاد کرده و خود را جای کسی که می‌شناسید و یا طرفدار او هستید جا زده تا بتواند شما را فریب دهد. و در نهایت اسمیشینگ (کلاهبرداری در قالب پیام‌های متنی) و فیشینگ (کلاهبرداری در قالب ایمیل) از دیگر انواع کلاهبرداری هستند.

بنابراین قبل از انجام خواسته دیگران، مانند کلیک کردن بر روی یک پیوند یا به اشتراک گذاری حساب کاربری خود، خوب است در مورد آن پیام چند سوال از خود بپرسید. در ادامه چندین پرسش را در اختیار شما قرار داده‌ایم که در چنین مواردی بایستی از خود پرسید:

- اگر پیام از سمت یک کسب و کار است، آیا حرفه‌ای به نظر می‌رسد و همچنین مارک تجاری آن محصول یا شرکت و متن ارسال شده حاوی اشتباهات املائی نیست.
- این که روی آدرس وبسایتی که در متن پیام برای شما ارسال شده است کلیک کنید، ایده خوبی نیست، بلکه بهتر است به مرورگر وب خود بروید، کسب و کار مذکور را جستجو کرده و سپس از خود بپرسید آیا URL سایت با نام محصول یا شرکتی که به دنبال آن هستید مطابقت دارد؟ آیا غلط املائی وجود دارد؟
- آیا پیام به شکل پنجره‌های پاپ‌آپ آزار دهنده ظاهر می‌شود؟
- آیا URL با `https://` و به همراه یک قفل سبز رنگ کوچک در سمت چپ آن شروع می‌شود؟ (که نشان دهنده اتصال ایمن است.)
- در متن چاپ شده با حروف ریز چه نوشته شده است؟ (گاهی کلاهبرداران در میان متن برخی تله‌های پنهانی می‌گذارند. البته اگر متن ریز هم وجود نداشته باشد هم نشانه خوبی نیست.)
- آیا پیام شامل موضوعی است که واقعی بودن آن دور از احتمال است، به طور مثال فرصتی برای کسب درآمد، دریافت یک شخصیت دیجیتالی بهتر برای آواتار خود، مشهور شدن و از این قبیل؟ (تقریباً آنقدر خوب است که درست بودنش شک‌برانگیز است.)
- آیا پیام عجیب به نظر می‌رسد؟ به طور مثال در پیام گفته شده است شما را می‌شناسند و شما نیز فکر می‌کنید ممکن است بشناسند، اما کاملاً مطمئن نیستید.

خوب، حال اگر گرفتار کلاهبرداری شدید چه اقداماتی باید انجام دهید؟ قبل از هر چیز نترسید! این موضوع خیلی رایج است. در اسرع وقت ماجرا را برای پدر یا مادر، معلم یا بزرگسال دیگری که به وی اعتماد دارید تعریف کنید. هر چه بیشتر تعلل کنید، ممکن است اوضاع بدتر شود.

- گذرواژه حساب‌های آنلاین خود را تغییر دهید.
- اگر مورد کلاهبرداری قرار گرفتید، فوراً به دوستان و آشنایان در فهرست مخاطبین خود اطلاع دهید، زیرا ممکن است آنها نیز چنین پیام‌هایی را دریافت کنند.
- در صورت امکان پیام را به عنوان هرزنامه گزارش دهید.

صلاحات ممکن برای کلاس‌های 2-3:

کلاس را به 5 گروه تقسیم کنید و یک نمونه از کاربرد را به هر گروه بدهید. به هر گروه فرصت دهید نمونه را تجزیه و تحلیل کند و سپس گفتگوی کلاسی را آغاز کنید

1. کلاس را تقسیم‌بندی کنید.

2. هر گروه نمونه‌ها را مطالعه کند.

کلاس به چند گروه تقسیم شده است و هر گروه نمونه پیام‌ها و وبسایت‌ها را مطالعه می‌کند.

3. افراد انتخاب می‌کنند.

برای هر نمونه بین «واقعی» یا «جعلی» بودن آنها انتخاب کرده و دلایل آن را در زیر آن فهرست‌وار بیاورید.

4. گروه‌ها درباره انتخاب‌های خود بحث می‌کنند.

کدام نمونه موثق و کدام یک شک برانگیز به نظر می‌رسد؟ آیا پاسخی داده شده است که برایتان جالب باشد؟ اگر چنین است علت را توضیح دهید.

فعالیت



وسایل مورد نیاز:

* توزیع شود: نمونه فیشینگ (پاسخ‌ها در صفحه 39)

• پاسخ به جزوه دانش‌آموزی:

«نمونه‌های فیشینگ»

1. **واقعی** پیام از کاربر می‌خواهد به‌جای ارائه پیوندی در پیام یا ارسال رمز عبور (پیوندها می‌توانند شما را به سمت وبسایت‌های مخرب بفرستند) به وبسایت شرکت رفته و وارد حساب کاربری خود شود.

2. **جعلی** URL مشکوک و ناایمن

3. **واقعی** به `https://` در URL توجه کنید.

4. **جعلی** پیشنهاد مشکوک در ازای اطلاعات بانکی

5. **جعلی** URL ایمن و مشکوک

6. **جعلی** URL ناایمن و مشکوک

7. **جعلی** آدرس اینترنتی مشکوک و ناایمن و پیشنهاد مشکوک در ازای اطلاعات بانکی

5. مباحث بیشتر

چند سؤال دیگر وجود دارد که باید به هنگام ارزیابی پیام‌ها و سایت‌های آنلاین از خود پرسید:

• آیا این پیام درست به نظر می‌رسد؟

حس غریزی شما چه می‌گوید؟ آیا متوجه برخی نکات شک‌برانگیز شده‌اید؟ آیا پیام حاوی پیشنهاد برطرف کردن مشکلی که خود از آن خبر نداشته‌اید، است؟

• آیا این برنامه درست به نظر می‌رسد؟

گاهی اوقات برنامه‌های جعلی که کاملاً شبیه برنامه‌های واقعی هستند در پاپ‌آپ‌های یک وبسایت تبلیغ شده و یا در فروشگاه‌های برنامه نمایش داده می‌شوند. در صورت دانلود کردن چنین برنامه‌هایی در تلفن همراه خود عواقب ناخوشایندی در انتظار شما خواهد بود. این برنامه‌ها اطلاعات شما یا مخاطبین شما را می‌دزدند، بدافزارهایی در تلفن یا دستگاه شما نصب می‌کنند و از این قبیل. مراقب اشتباهات املایی، تعداد کم نظرات کاربران یا گرافیک‌های درهم (نه چندان حرفه‌ای) باشید.

• آیا در پیام چیزی رایگان به شما پیشنهاد شده است؟

پیشنهادات رایگان در عمل رایگان نیستند و فرستندگان اغلب در قبال آن چیزی از شما دریافت می‌کنند.

آیا اطلاعات شخصی شما را می‌خواهد؟

برخی کلاهبرداران اطلاعات شخصی را درخواست کرده تا بتوانند شما را در معرض کلاهبرداری‌های بیشتر قرار دهند. برای مثال آزمون‌ها یا «تست‌های شخصیتی» ممکن است حقایقی را در مورد شما جمع‌آوری کنند تا بدان وسیله رمز عبور یا سایر اطلاعات مخفی شما را حدس بزنند. اکثر مشاغل واقعی به جز در وبسایت خود هرگز اطلاعات شخصی شما را در قالب یک پیام یا فرم درخواست نمی‌کنند.

آیا این پیامی زنجیره‌ای است یا پستی اجتماعی؟

متن‌ها و پست‌هایی که از شما می‌خواهند آن‌ها را برای هر کسی که می‌شناسید ارسال کنید، می‌تواند شما و دیگران را در معرض خطر قرار دهد. این کار را انجام ندهید، مگر این که منبع فرستنده آن را شناخته و مطمئن باشید انتقال پیام بی‌خطر است.

آیا متن چاپ شده با حروف ریز نیز وجود دارد؟

در پایین اکثر اسناد «متن چاپ شده با حروف ریز» را خواهید یافت. این متن کوچک بوده و اغلب حاوی مطالبی است که ممکن است از قلم افتاده باشند. به طور مثال ممکن است در بالای صفحه گفته شده باشد که شما برنده یک دستگاه تلفن همراه رایگان شده‌اید، اما در متن چاپ شده با حروف ریز خواهید خواند باید 200 دلار در ماه به آن شرکت پرداخت کنید. تمام این متون ریز به آن اندازه که به نظر می‌رسند، بد نیستند، پس حتماً آنها را با دقت بخوانید.

دقت کنید: برای دستیابی به هدف این تمرین، فرض کنید ایمیل Internaut یک سرویس واقعی و قابل اعتماد است.

نکته

نکته: وقتی آنلاین هستید مراقب باشید در بازی‌ها، صفحات وب، برنامه‌ها و پیام‌ها مورد کلاهبرداری قرار نگیرید و بدانید که هر پیام وسوسه‌انگیزی یا ارائه هرچیز رایگانی به احتمال زیاد جعلی بوده و در صورتی که در دام این کلاهبرداری‌ها افتادید به سرعت بزرگسال مورد اعتماد خود را در جریان قرار دهید.

نمونه‌های فیشینگ

1. آیا این متن واقعی است یا ساختگی؟



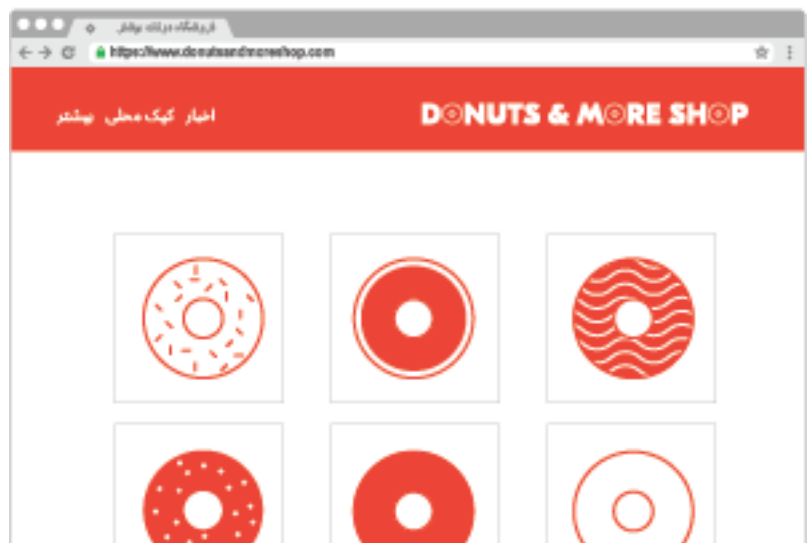
ساختگی . واقعی.

2. آیا این واقعی است یا ساختگی؟



ساختگی . واقعی.

3. آیا این واقعی است یا ساختگی؟



ساختگی . واقعی.

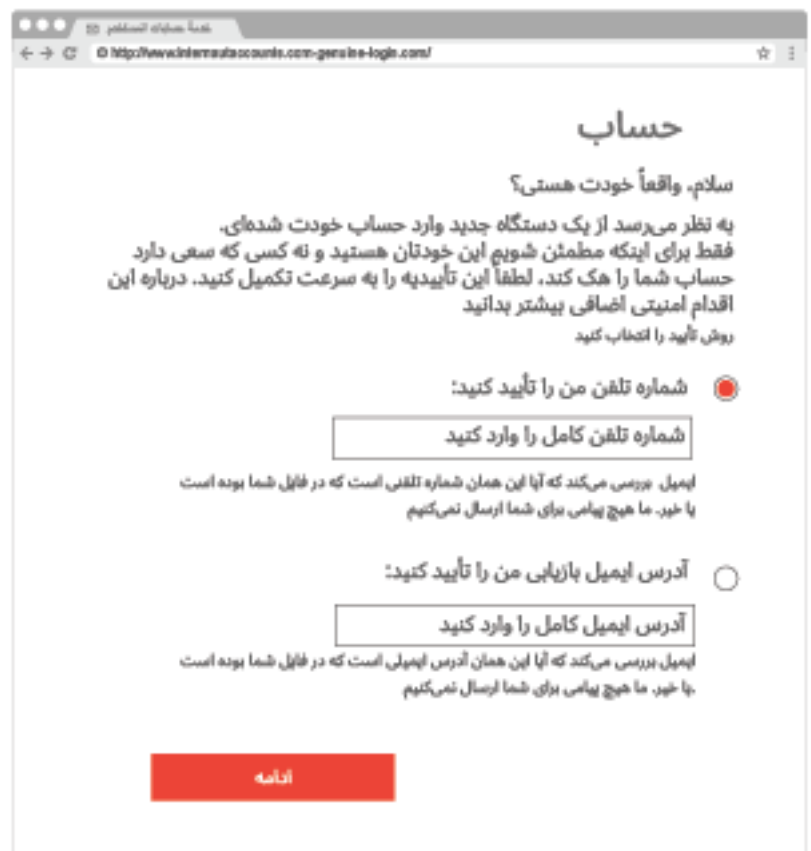
4. آیا این واقعی است یا ساختگی؟

ساختگی . _____
واقعی . _____



5. آیا این واقعی است یا ساختگی؟

ساختگی . _____
واقعی . _____



6. آیا این واقعی است یا ساختگی؟

ساختگی .
واقعی.



7. آیا این واقعی است یا ساختگی؟

ساختگی .
واقعی.



دانش‌آموزان مهارت خود در مبارزه با کلاهبرداری را با نمایش و گفتگو در خصوص پاسخ‌های احتمالی به پیام‌های آنلاین، پست‌ها، درخواست‌های دوستی، برنامه‌ها، تصاویر و ایمیل‌های مشکوک تمرین می‌کنند.

درباره این درس: از آنجایی که این درس در مورد تعامل اجتماعی است، می‌تواند برای دانش‌آموزان پایه‌های ابتدایی (5-6) مناسب باشد، اما از آنجا که کودکان 7 تا 9 ساله بیشتر به بازی‌های آنلاین می‌پردازند و بسیاری از آنها بازی گروهی را به بازی انفرادی ترجیح می‌دهند، این درس برای کلاس‌های 2-3 نیز آماده سازی خوبی به حساب می‌آید. امیدواریم معلمان این پایه‌های تحصیلی متوجه شوند آیا دانش‌آموزانشان به چنین بازی‌هایی می‌پردازند یا خیر، و اگر چنین است، چه چیز در این بازی‌ها را دوست دارند و آیا تا به حال موردی غیر عادی را تجربه کرده‌اند یا خیر. به منظور بهبود هرچه بیشتر یادگیری، بایستی این تمرین‌ها را ساده، شفاف و بدون هیچ گونه قضاوتی انجام داد.

اهداف درس برای دانش‌آموزان للطلاب:

- ✓ درک این نکته که افرادی که با آنها تماس می‌گیرند ممکن است همانی نباشند که می‌گویند.
- ✓ قبل از پاسخ دادن مطمئن شوند شخص همان کسی است که وانمود می‌کند.
- ✓ اگر تشخیص هویت شخص مشکل است، سؤال پرسیده یا از یک بزرگسال کمک بگیرید.



چگونه می‌فهمید آنها همانی هستند که می‌گویند؟

وقتی تلفنی با دوست خود صحبت می‌کنید، از صدایش متوجه می‌شوید او چه کسی است؛ حتی اگر نتوانید تصویرش را ببینید. دنیای آنلاین کمی متفاوت است. گاهی اوقات اطمینان از این که دیگران همان کسی هستند که وانمود می‌کنند، دشوار است. برنامه‌ها و بازی‌ها گاهی برای برخی شوخی و سرگرمی خود را جای شخص دیگری وانمود کرده تا چیزی از شما بگیرند و یا شما را اذیت کنند. گاهی نیز آنها به منظور سرقت اطلاعات شخصی یا دارایی دیجیتالی شما مانند دارایی یا سکه‌های بازی هویت خود را جعل می‌کنند. مطمئن‌ترین راهکار این است که هیچ پاسخی به آنها ندهید و یا به والدین یا بزرگسال دیگری که به وی اعتماد دارید اطلاع دهید فردی ناشناس سعی در برقراری ارتباط با شما دارد. اما اگر به این نتیجه رسیدید که جواب دادن اشکالی ندارد، بهترین کار این است که ابتدا در مورد وی اطلاعات کسب کنید. صفحه یا نمایه فرد را بررسی کنید، ببینید دوستان وی چه کسانی هستند یا اطلاعات دیگری را جستجو کنید که به شما می‌گوید او همان کسی است که می‌گوید یا خیر.

بیا یاد حرف بزنیم



راه‌های زیادی برای تأیید هویت شخصی آنلاین وجود دارد. در اینجا چند مثال برای شروع کار آورده شده است.

نکته برای معلم:

ابتدا در این مورد که «چگونه هویت یک فرد را در اینترنت تأیید کنیم؟» یک گفتگوی کلاسی راه بیان‌دازد و سپس گفتگو در مورد این ایده‌های فکری را ادامه دهید.

• اگر عکسی از فرستنده پیام وجود داشته باشد، بازم باید مشکوک بود؟

آیا عکس وی تار است یا به سختی قابل روئت است و یا در کل عکس او مانند چهره یک شخصیت کارتونی یا بیت‌موجی است؟ عکس‌های نامشخص، بیت‌موجی‌ها، عکس حیوانات خانگی و غیره باعث می‌شود شخص به راحتی هویت خود را در شبکه‌های اجتماعی پنهان کند. همچنین برای کلاهبرداران کاری ندارد عکس‌های شخصی واقعی را به منظور ایجاد یک نمایه جعلی سرقت کنند. اگر عکسی وجود دارد، آیا می‌توانید عکس‌های بیشتری از فرد با آن نام در اینترنت پیدا کنید؟

• آیا نام صفحه نمایش آنها حاوی نام واقعی آنها است؟

به عنوان مثال در رسانه‌های اجتماعی نام صفحه نمایش آنها با نام واقعی آنها مطابقت دارد؟ (به عنوان مثال نمایه جین دو دارای یک URL مانند SocialMedia.com/jane_doe است.)

• آیا صفحه آنها حاوی اطلاعاتی در مورد آنها است؟

اگر چنین باشد، آیا به نظر می‌رسد این اطلاعات توسط شخصی حقیقی نوشته شده است؟ حساب‌های جعلی ممکن است اطلاعات زیادی در بخش «درباره من» نداشته باشند، یا ممکن است دسته‌ای از اطلاعات کپی شده یا به‌طور تصادفی کنار هم جمع شده باشند تا یک نمایه جعلی ایجاد کنند. آیا چیزی در اطلاعات آنها وجود دارد که با جستجوی نام در نمایه بتوانید آن را تأیید کنید؟

• حساب فرد مذکور از چه زمان فعال است؟ آیا فعالیت وی مشخص است؟

آیا صفحه فرد مذکور یا نمایه وی جدید است، یا فعالیت‌های زیادی از گذشته را در خود دارد؟ آیا آن شخص با شما دوستان مشترکی دارد؟ حساب‌های جعلی معمولاً محتوای زیادی ندارند یا نشانه‌ای از محتواها، نظرات و دوستی با افراد دیگر در آنها وجود ندارد.

فعالیت



مواد مورد نیاز:

• کاربرگ «مخاطب من چه کسی است؟» را به شکل نوار برش دهید به طوری که هر برش حاوی یک سناریو باشد.

• کاسه یا ظرف برای گذاشتن بریده‌ها در آن (هر گروه از دانش‌آموزان یکی را انتخاب می‌کند).
ورقة غش التصيد الاحتيالي

• طرح کلی دانش‌آموز مندرج در صفحه 46 (یکی برای هر دانش‌آموز).

1. گروه سناریوها را بررسی می‌کند.

خوب، حال به 5 گروه تقسیم شده و هر گروه سناریویی را از درون ظرف برمی‌دارد.

2. هر گروه یک یا چند پاسخ را از میان فهرست موجود انتخاب کرده و در مورد این که چرا بایستی چنین پاسخی را به موقعیت مورد نظر داد، صحبت می‌کند. در نوشتن پیام‌های بیشتری که فکر می‌کنید پیچیدگی بیشتری دارند، آزادانه عمل کنید.

3. کلاس درباره انتخاب‌های گروه بحث می‌کند.

در نهایت اجازه دهید از فهرست پاسخ‌های موجود برای مباحث کلاسی در مورد تمامی سناریوها استفاده شود. هر گروه سناریویی خود را خوانده و به کلاس در مورد پاسخ خود و دلیل انتخاب آن (یا آن‌ها) توضیح می‌دهد. کلاس در این مورد گفتگو می‌کند.

نکته

باید بدانید در اینترنت با چه کسانی صحبت می‌کنید. مطمئن شوید کسی که با وی در اینترنت ارتباط برقرار می‌کنید، همانی است که می‌گویید!

«مخاطب من چه کسی است؟»

سناریو 1

درخواست دوستی از سوی یک بازیکن ناشناس را در طی یک بازی آنلاین دریافت می‌کنید به این مضمون: «سلام، خوبی! می‌آیی با هم بازی کنیم! من را اضافه می‌کنی؟»

سناریو 2

یک پیام متنی در تلفن همراه خود از شخصی که نمی‌شناسید دریافت می‌کنید: «سلام، من کوری هستم! یادت هست تابستان پارسال با هم آشنا شدیم؟»

سناریو 3

از شخصی که جزو دوستانتان نیست پیامی دریافت می‌کنید: «سلام! از محتواهایی که می‌گذاری خوشم می‌آید، خیلی بانمک هستی! شماره تلفنت را به من بده تا بیشتر صحبت کنیم!»

سناریو 4

این متن از سوی فردی که نمی‌شناسید برای شما ارسال شده است: «امروز تو را در سالن دیدم، تو خیلی نازی! آدرست کجاست؟ می‌توانم دور و بر ساعت 2 پیام و تو را ببینم.»

سناریو 5

شما یک پیام آنلاین دریافت می‌کنید: «سلام، من به تازگی دوستت سام را دیدم! او در مورد تو برایم تعریف کرد. می‌خواهم تو را ببینم. کجا زندگی می‌کنی؟»

طرح کلی دانش‌آموز: درس 2

«مخاطب من چه کسی است؟»

پنج سناریو شامل پیامهایی که هر کس ممکن است به صورت آنلاین یا در تلفن خود دریافت کند، آورده شده است. همچنین راه‌هایی وجود دارد که می‌توانید برای پاسخ دادن به این پیام‌ها از آن‌ها استفاده کنید، برخی از این پاسخ‌ها عالی و برخی دیگر نه چندان خوب هستند. ببینید کدام یک (یادو مورد) برای شما منطقی‌تر است و یا اگر پاسخ‌های دیگری در نظر دارید، بگویید. حال در مورد این پاسخ‌ها صحبت کنید، و در نهایت بحث کلاسی خواهیم داشت.

همه لطفاً توجه داشته باشند: اگر یکی از این سناریوها در زندگی واقعی اتفاق بیافتد و شما ندانید چه کار باید انجام دهید، ساده‌ترین کار پاسخ ندادن است. همیشه می‌توانید چنین مواردی را نادیده بگیرید یا فرستنده آن‌ها را مسدود کنید. صحبت کردن با والدین یا معلم در مورد چنین پیامهایی هیچ ضرری ندارد، بخصوص اگر این پیام‌ها باعث آزاد شما هستند.

سناریوی 1

شما یک درخواست دوستی از یک بازیکن ناشناس در یک بازی دریافت می‌کنید: «سلام، خوبی! می‌آیی با هم بازی کنیم! من را به دوستانت اضافه کن.» چه می‌کنید؟

• **آن را نادیده می‌گیرید.** اگر آنها را نمی‌شناسید، می‌توانید آنها را به دوستان خود اضافه نکنید.

• **آنها را مسدود کنید.** دیگر پیامی از آنها در دیگر بازی‌ها یا برنامه‌ها دریافت نخواهید کرد و آنها نیز متوجه نمی‌شوند که شما آنها را مسدود کرده‌اید.

• **تنظیمات خود را تغییر می‌دهید.** به قسمت تنظیمات بازی بروید، ببینید آیا می‌توانید دریافت درخواست‌های دوستی را خاموش کنید و آن کادر را علامت بزنید. به این ترتیب مجبور نخواهید بود در مورد پذیرش یا عدم پذیرش درخواست‌های بازیکنان تصادفی تصمیم بگیرید.

• **آنها را بررسی کنید.** ببینید آیا آنها صفحه یا نمایه‌ای دارند که بتوان فهمید آیا آن‌ها واقعاً بازیکن هستند یا خیر. آیا آن‌ها هیچ محتوا یا دنبال کننده‌ای دارند؟ آیا دوستان آنها را می‌شناسند؟ اگر به نظر رسید که آنها یک بازیکن واقعی هستند، بعد می‌توانید در مورد پذیرش دوستی آنها تصمیم بگیرید. اما واقعاً بهترین کار برای بچه‌ها این است که فقط با دوستان آفلاین خود بازی کنند.

• **آنها را به فهرست دوستان خود اضافه کنید.** شاید این کار خوب به نظر برسد، اما توصیه نمی‌شود، مگر این که بدانید چه کسی هستند و یا از بزرگسالی که به وی اعتماد دارید یا حداقل دوستانتان کمک خواسته و بررسی کنید آیا آنها می‌دانند این شخص کیست یا خیر. اگر با آن‌ها از طریق میکروفون یا هدست بازی می‌کنید، فقط در مورد بازی حرف بزنید و هرگز نام کامل یا اطلاعات شخصی خود را به اشتراک نگذارید.

• **اطلاعات شخصی خود را به آنها بدهید.** قطعاً این کار درستی نیست. شما هرگز نباید اطلاعات شخصی را در اختیار افرادی که نمی‌شناسید، قرار دهید.

سناریوی 2

از طرف شخصی که نمی‌شناسید پیامی به این مضمون دریافت می‌کنید: «سلام، من کوری هستم! یادت هست تابستان پارسال با هم آشنا شدیم؟ چطوری؟»

• **کوری را مسدود بگیرید.** اگر واقعا او را بشناسید این کار بی‌ادبانه است. اما اگر مطمئن هستید که تابستان گذشته کسی به نام کوری را ملاقات نکرده‌اید یا او پیامک‌های زیادی برای شما ارسال می‌کند و در مورد خود بیش از حد مطلب به اشتراک می‌گذارد، بهتر است او را مسدود کنید.

• **کوری را نادیده می‌گیرید.** همانطور که در بخش فوق هم گفتیم، اگر این شخص را نمی‌شناسید، بهترین کار پاسخ ندادن به پیام او است.

سلام، کوری. من را از کجا یادت هست؟ اگر مطمئن نیستید که چنین فردی را ملاقات کرده‌اید یا خیر و می‌خواهید با کمی اطلاعات بیشتر بفهمید آیا او را دیده‌اید، این پرسش یک گزینه مطمئن است. اما به کوری نگویند تابستان گذشته کجا بوده‌اید!
من شما را به خاطر نمی‌آورم، اما با این حال می‌توانیم گاهی اوقات همدیگر را ملاقات کنیم. به هیچ وجه ایده خوبی نیست؛ هرگز نباید پیشنهاد ملاقات با کسی که نمی‌شناسید را بدهید.

شما از فردی با نام کاربری @soccergirl12 پیامی دریافت می‌کنید. او جزو دنبال شونده‌گان (فالورهای) شما نیست. پیام به این مضمون است: «سلام! محتواهای تو را دوست دارم، تو خیلی بانمک! شماره تلفنت را بده تا بیشتر صحبت کنیم!» در این صورت چه می‌کنید؟

• **soccergirl12 را نادیده بگیرید.** لیس عليك الرد إذا كنت لا تريد ذلك.

• **@soccergirl12 را مسدود می‌کنید.** اگر این شخص به نظرتان ناشناس و عجیب و غریب است او را بلاک کنید، در این صورت هرگز هیچ پیامی از او نخواهید گرفت، مگر این که یک نمایه جعلی جدید راه‌اندازی کند و به عنوان یک فرد جعلی جدیدی با شما تماس بگیرد.

• **«سلام، من شما را می‌شناسم؟».** اگر مطمئن نیستید، قبل از دادن هرگونه اطلاعات شخصی مانند شماره تلفن حتماً این سؤال پرسید.

• **«خوب، این شماره من است.»** نه! حتی اگر بدانید او کیست، ارائه اطلاعات شخصی از طریق رسانه‌های اجتماعی ایده خوبی نیست. راه دیگری برای تماس پیدا کنید، خواه از طریق والدین، معلم یا شخص مورد اعتماد دیگری باشد.

این متن از کسی که نمی‌شناسید برای شما ارسال می‌شود: «امروز تو را در سالن دیدم. تو خیلی نازی! آدرست چیست؟ می‌توانم دور و بر ساعت 2 بیایم و تو را ببینم.»

• **او را نادیده می‌گیرید.** به احتمال زیاد انتخاب خوبی است

• **این شخص را مسدود کنید.** اگر احساس بدی نسبت به کسی پیدا کردید از این کار هیچ ابایی نکنید.

• **«شما چه کسی هستید؟».** احتمالاً گزینه خوبی نیست. بهتر است هرگز به هیچ پیام مشکوک پاسخ ندهید و یا خیلی ساده، شخص فرستنده را مسدود کنید.

• **«تو لیزی هستی؟ تو هم ناز هستی! من در سیراکل، شماره 240 زندگی می‌کنم.»** این کار به هیچ وجه ایده خوبی نیست، حتی اگر فکر می‌کنید می‌دانید او چه کسی است. قبل از این که آدرس یا هر اطلاعات شخصی دیگری را به کسی بدهید، او را بررسی کنید، حتی اگر فکر می‌کنید او را می‌شناسید. هرگز شخصی را که فقط از طریق گفتگوی آنلاین می‌شناسید ملاقات نکنید.

سناریوی 3

سناریوی 4

سناریوی 5

شما پیام آنلاین به این مضمون دریافت می‌کنید: «سلام، من به تازگی دوستت سام را دیدم! او در مورد تو برایم تعریف کرد. دوست دارم تو را ببینم. کجا زندگی می‌کنی؟»

• **او را نادیده می‌گیرید.** اگر این شخص را نمی‌شناسید اما دوستی به نام سام دارید، بهترین کار این است که قبل از پاسخ دادن به این پیام ابتدا با سام مشورت کنید.

• **او را مسدود می‌کنید.** اگر این شخص را نمی‌شناسید و دوستی به نام سام ندارید، بهترین کار این است که از تنظیمات خود برای جلوگیری از تماس بیشتر این شخص با خود استفاده کنید.

• **«شما چه کسی هستید؟»** احتمالاً ایده خوبی نیست. اگر آن شخص را نمی‌شناسید، بهتر است حداقل تا زمانی که از سام در این مورد نپرسیده‌اید، به او پاسخ ندهید.

به دام کلاهبردارها نیفتید: درس 3 آیا این واقعا درست است؟

پیشینه سواد رسانه‌ای برای معلمان: علاوه بر کمک به دانش‌آموزان خود در راستای استفاده از پرسش‌های تحلیلی به منظور ارزیابی اعتبار منبع، می‌خواهیم آنها به این درک برسند که اطلاعات از منابع بسیار (نه فقط کتاب‌های درسی) به دست می‌آیند. بنابراین آنها باید مهارت‌های خود را در راستای تجزیه و تحلیل انواع رسانه‌ها به کار گیرند. وقتی به این نقطه رسیدند، آماده هستند تا دسته‌بندی‌های خاص رسانه‌ها مانند اخبار یا داده‌های علمی را مورد تجزیه و تحلیل قرار دهند.

توجه: این درس در مورد سواد رسانه‌ای است که می‌تواند برای همگان مفید باشد، اما ممکن است کمی فراتر از سطح دانش‌آموزان کلاس‌های 2 تا 3 باشد، بنابراین اصلاحیه پیشنهادی مندرج در بخش «فعالیت» را مشاهده نمایید.

اهداف درس برای دانش‌آموزان



- ✓ **شناسایی** ابزارهایی که بیشتر به منظور اعتبارسنجی اطلاعات به کار می‌برند.
- ✓ **در نظر گرفتن** این نکته که چگونه برخی موارد خاص مانند تخصص و انگیزه بر اعتبار تأثیر می‌گذارند.
- ✓ **آموختن** چهار سوال اساسی برای ارزیابی اعتبار منبع.
- ✓ **درک** این که اعتبار منبع در یک موضوع، لزوماً باعث اعتبار آن منبع در دیگر موضوعات نمی‌شود.
- ✓ **این که** بررسی چندین منبع به منظور شناسایی معتبر بودن اطلاعات مفید است.

پایید حرف بزنیم



چه چیز به موضوعات یا اشخاص اعتبار و اطمینان می‌بخشد؟

هر روز تصمیم می‌گیرید چه چیز را باور کنید یا باور نکنید. آن فیلمی که دیدی راست بود؟ آیا فیلم قصد داشت شما را به انجام کاری وادار سازد؟ آیا برادر بزرگتر شما حقیقت را می‌گوید یا مسخره بازی در می‌آورد؟ آیا آن شایعه‌ای که در مورد یکی از دوستانتان شنیدید، حقیقت داشت؟

وقتی می‌خواهید تصمیم بگیرید که آیا کسی حقیقت را می‌گوید یا خیر چه می‌کنید؟ آیا از این سرخ‌ها استفاده می‌کنید؟

• آنچه در مورد شخص می‌دانید.

برای مثال می‌دانید همکلاسی شما واقعا در کاری خوب است یا سابقه راستگویی یا سربه سر گذاشتن دیگران یا بداخلاقی را دارد، بنابراین با بررسی این موارد می‌توانید تشخیص دهید همکلاسی شما چه زمان جدی است یا شوخی می‌کند یا دروغ می‌گوید.

• آنچه شخصی در مورد شما می‌داند.

به عنوان مثال والدین شما به خوبی می‌دانند چه غذاهایی باعث دل درد شما می‌شود. تبلیغات تلویزیونی اینگونه نیستند، بنابراین در این مورد به توصیه والدین خود عمل می‌کنید. کتابدار مدرسه از علائق شما و نوع کتاب‌هایی که دوست دارید با خبر است، بنابراین به توصیه‌های او در مورد انتخاب کتاب اعتماد دارید.

• لحن صدا و حالت چهره.

برای مثال می‌دانید اگر دوستان چشم‌هایش را بچرخاند و با طعنه بگوید در پارک جدید به او خوش نگذشته است، منظورش برعکس است.

• موقعیت.

به طور مثال وقتی با دوستان بازی می‌کنید و یکی از آنها شما را به خاطر مدل موی جدیدتان دست می‌اندازد، می‌دانید که این فقط یک شوخی است. اما اگر کسی در مدرسه دقیقا همین کلمات را عنوان کند تا شما را جلوی کل کلاس شرمند نماید، یک توهین محسوب می‌شود.

وقتی چیزهایی را از یک منبع رسانه‌ای مانند فیلم، تلویزیون یا وب سایت می‌شنویم، شخصا منبع را نمی‌شناسیم و آنها نیز ما را نمی‌شناسند، از این رو نمی‌توانیم به سخنان آنها اطمینان کنیم.

حتی وقتی کسی که می‌شناسیم برای ما پیامی می‌فرستد، هیچ سرنخی از حالات چهره یا لحن صدای وی وجود ندارد، بنابراین ممکن است در مورد منظور وی مطمئن نباشیم. این موقع است که باید سوال پرسیم.

اصلاحات توصیه شده برای کلاس‌های 2-3:

اگر احساس می‌کنید دانش‌آموزان شما آماده بحث در مورد معتبر بودن منبع هستند، فقط مراحل 1 و 2 را کامل کنید.

1. ارزیابی منابع.

اگر دنبال یک بازی ویدیویی جدید و عالی باشید، از مادربرگتان می‌خواهید شما را در این زمینه راهنمایی کند؟ یا به بیانی دیگر، آیا مادربرگ شما منبع معتبری از اطلاعات در مورد بازی‌های ویدیویی است؟ منبع معتبر منبعی است که مطمئن باشیم اطلاعات دقیق و مرتبطی به ما خواهد داد.

برای توضیح مزایا و معایب درخواست مشاوره از مادربرگتان برای بازی‌های ویدیویی، فهرستی شامل معایب و مزایای این کار تهیه کنید.

آیا فهرست تهیه شده چیزی شبیه به این فهرست است؟

مزایا	معایب
مادربرگم من را دوست دارد و می‌خواهد خوشحال باشم	مادربرگ بازی ویدیویی بازی نمی‌کند و چیزی در این داندباره نمی‌داند
مادربرگ حتی اگر خودش جواب را نداند، اما در یافتن اطلاعات بسیار خوب عمل می‌کند	مادربرگ نمی‌داند کدام بازی‌ها را دارم یا چه نوع بازی‌هایی را دوست دارم

اگر فهرست شما اینگونه باشد، پس شما تنها از دو مورد از رایج‌ترین ابزارها به منظور تصمیم‌گیری در مورد موثق بودن یک منبع استفاده کرده‌اید: انگیزه و تخصص. «تخصص» مهارت یا دانشی ویژه در مورد یک موضوع خاص است. کارشناسان از تخصص یا دانش ویژه در مورد یک موضوع خاص برخوردار هستند. «انگیزه» به معنای قصد و نیت است، دلیل این که فرد چیزی می‌گوید یا کاری انجام می‌دهد.

کدام مورد در فهرست شما اطلاعاتی در مورد انگیزه مادربرگ به شما می‌دهد؟ کدام موارد چیزی در مورد تخصص او می‌گوید؟ آیا مادربرگ در نمودار مزایا/ معایب منبعی معتبر برای کسب اطلاعات در مورد بازی ویدیویی جدید است؟ او دروغ نمی‌گوید، اما در این شرایط بهتر است این سوال را از کسی پرسیم که علاوه بر این که به ما اهمیت می‌دهد، درباره بازی و انواع بازی‌هایی که ما دوست داریم نیز اطلاع دارد.

فعالیت



• وسائل مورد نیاز:

- جزوه: «تصمیم‌گیری در این خصوص که چه چیز معتبر است» (یکی برای هر دانش‌آموز)

ممکن است پدرمان آشپز فوق‌العاده‌ای باشد، اما از مد اطلاعی نداشته باشد، مربی ما بسکتبال بلد است، اما در ژیمناستیک سررشته‌ای ندارد، یا این که مادر بزرگ می‌تواند تقریباً هر اسباب‌بازی را درست کند، اما چیزی در مورد بازی‌های ویدیویی نمی‌داند. این که فردی در یک چیز تخصص دارد، باعث نمی‌شود که او در همه چیز متخصص باشد.

2. فهرست مزایا و معایب خود را تهیه کنید.

اگر اولین بار است که فکر می‌کنید چگونه از انگیزه و تخصص به عنوان سرنخ استفاده کرده تا بتوانید در مورد اعتبار منابع اطلاعاتی تصمیم بگیرید، ممکن است به تمرین بیشتر نیاز داشته باشید.

تصور کنید قصد دارید بفهمید چگونه فوتبالیستی بهتر شوید. برای این کار بهتر است فهرست مزایا/معایبی را ایجاد کنید تا بتوانید تصمیم بگیرید آیا منابع مورد نظر شما منابع معتبری هستند یا خیر:

- مادر بزرگ شما
- وبلاگی که توسط مربی بسکتبال دبیرستان برنده اداره می‌شود.
- بهترین بازیکن تیم.
- وبسایتی که کفش ورزشی می‌فروشد و در این مورد مشاوره می‌دهد.
- ویدئوهایی که تکنیک‌های تمرین فوتبال را آموزش می‌دهند.

- در مورد نقاط قوت و ضعف هر منبع باید چه چیزهایی را در نظر داشته باشید؟
- آیا کسی هست که نحوه تدریس را بلد باشد، اما با مهارت‌های فوتبال آشنا نباشد؟
 - آیا کسی وجود دارد که متخصص فوتبال باشد؛ اما نداند چگونه تدریس کند؟
 - آیا کسی وجود دارد که همیشه پیشنهادش پیرامون خرید چیزی باشد؟
 - آیا کسی هست که فوتبال بلد باشد، اما شما را نشناسد یا نداند باید بر روی کدام مهارت خود بیشتر کار کنید؟

گفتگو: منبع خوب چه کسی است و چرا چنین فکر می‌کنید؟

اعتبار داشتن همیشه به معنای همه یا هیچ نیست. اکثر منابع دارای نقاط قوت و ضعف هستند، به همین دلیل شاید بهترین پاسخ‌ها اغلب با طرح پرسش از منابع بسیار و مقایسه پاسخ‌های آنها به دست آید.

2. مراحل که باید در نظر بگیرید.

اعتبار تنها به این معنی نیست که به چه کسی باور داریم، بلکه به معنای چیزی که به آن باور داریم نیز است. همه چیز و همه جا در مورد دنیا ایده‌هایی در اختیار ما قرار داده و فقط انسان‌ها نیستند که چنین ایده‌هایی را در اختیار ما می‌گذارند. در فیلمی یک سونامی غول پیکر که بسیار عظیم‌تر از یک آسمان‌خراش بود نشان داده شد که در حال نزدیک شدن به مردمی بود که در ساحل بودند. آیا سونامی واقعا این شکلی است؟ یک آگهی تبلیغاتی نشان می‌داد که اکثر دانشمندان مردانی با موهای ژولیده هستند و همیشه عینک‌های ضخیم به چشم داشته و لباس سفید آزمایشگاهی می‌پوشند. آیا چنین چیزی درست است؟

ما می‌توانیم با استفاده از 3 مرحله تصمیم‌گیری درباره آنچه که مورد اطمینان و اعتبار است هر منبعی را بررسی کنیم. این سه مرحله پیرامون همان تخصص و انگیزه می‌چرخند.

مرحله 1: از عقل سلیم استفاده کنید

پرسید: آیا منطقی است، آیا معقولانه است؟

اگر الف چیزی که می‌بینید منطقی نباشد، ب بر اساس تجربه می‌دانید که درست نیست، یا ج با حقایقی که بیشتر می‌دانستید همخوانی ندارد، لازم نیست مرحله دیگری پیش بروید. این منبع نامعتبر است.

مرحله 2: سوال پرسید.

نه هر سوالی، بلکه این چهار سوال:

تخصص

الف) آیا این منبع من را می‌شناسد یا به من اهمیت می‌دهد؟

پاسخ به این سوال به اطلاعاتی که به دنبال آن هستید بستگی دارد. اگر در حال بررسی اطلاعاتی در مورد بطری‌های پلاستیکی هستید که اقیانوس‌ها را آلوده می‌کنند، مهم نیست که منبع شما را می‌شناسد یا نه. اما اگر سایتی قول می‌دهد که شما عاشق اسباب‌بازی جدید آن‌ها خواهید شد، باید بدانید که شما از چه نوع اسباب‌بازی‌ها، بازی‌ها یا فعالیت‌هایی خوشتان می‌آید تا قولشان معتبر باشد.

ب) آیا این منبع اطلاعات زیادی در مورد موضوع دارد؟ آنها این اطلاعات را از کجا به دست آورده‌اند؟

می‌کنند ساده‌ترین راه برای یافتن اطلاعات معتبر این است که از دستیار صوتی دیجیتال سوال پرسند. به نظر می‌رسد دستیارهای دیجیتال همه چیز را می‌دانند! آیا تا به حال به این موضوع اندیشیده‌اید که آن‌ها چگونه این پاسخ‌ها را میداند؟ آنها از محاسبات ریاضیاتی (به نام الگوریتم) برای یافتن پاسخ استفاده می‌کنند.

دستیارهای دیجیتالی برای سؤالات ساده‌ای که فقط یک پاسخ ممکن دارند (مانند دمای بیرون یا نام یک سلبریتی معروف که یک آهنگ پاپ خاص خوانده است) منبع معتبری به حساب می‌آیند. اما اگر سوال پیچیده باشد، بهتر است آن را از افراد یا گروه‌هایی که تجربه بسیاری در این مورد دارند یا جوایزی در مورد موضوع مورد نظر شما کسب کرده‌اند و یا در این زمینه دکترا دارند پرسید. سپس می‌توانید از یک دستیار صوتی برای تأیید آن اطلاعات استفاده کنید (مرحله 3 را ببینید).

انگیزه

ج) منبع از من می‌خواهد چه کاری انجام دهم یا چه چیز را باور کنم و چرا آنها از من می‌خواهند که این کار را انجام دهم یا این موضوع را باور کنم؟

آیا تبعیت از توصیه‌های آنها باعث کسب درآمد آنها می‌شود؟ به عنوان مثال آیا فکر می‌کنید یک اینفلوئنسر (شاخ مجازی) در صورت خرید محصولی که می‌پوشد یا درباره آن صحبت می‌کند، هزینه‌ای دریافت می‌کند؟ آیا یک ورزشکار حرفه‌ای مارک خاصی از کفش یا پیراهن را فقط به این دلیل می‌پوشد که آن مارک را دوست دارد یا به این دلیل که برای صحبت در مورد آن پول می‌گیرد؟

پول اغلب یکی از دلایلی است که یک لوگو یا نام تجاری را در یک ویدیو یا تبلیغ می‌بینید و می‌تواند بر آنچه اینفلوئنسر یا ورزشکار به شما می‌گوید (و آنچه به شما نمی‌گوید) تأثیر بگذارد. البته به احتمال زیاد آنها قصد ندارند به شما صدمه بزنند، اما این امکان وجود دارد که پول درآوردن برای آنها مهم‌تر از ارائه تمام حقایق یا گفتن آنچه برای شما خوب است، باشد.

د) اگر مردم این منبع را باور کنند چه کسی سود برده و چه کسی ممکن است آسیب ببیند؟

گفتن این موضوع همیشه آسان نیست. به یک مثال توجه کنید:

تبلیغ یک برنامه رایانه‌ای را تصور کنید که در آن به شما قول می‌دهند شما را تبدیل به دانش‌آموز بهتری کنند.

• مزایای احتمالی این برنامه چیست؟ اگر برنامه را بخرید سازنده سود خواهد برد، زیرا پول در می‌آورد و اگر برنامه واقعا به شما کمک کند، شما نیز ممکن است سود ببرید.

• اگر تبلیغ را باور کنید چه کسی ممکن است آسیب ببیند؟ اگر برنامه را بخرید ممکن است پول خود را هدر دهید. همچنین ممکن است وقت خود را صرف تمرین چیزهای اشتباه کنید، و حتی عملکرد بدتری در مدرسه پیدا کنید و یا این امکان وجود دارد که به جای کمک گرفتن از معلم خود، که در واقع می‌داند به چه چیز نیاز دارید، به برنامه تکیه کنید، که فقط می‌تواند در مورد آنچه نیاز دارید حدس بزند.

مرحله 3: تایید

بپرسید: آیا منابع معتبر دیگر از گفته‌های این منبع پشتیبانی می‌کنند؟

کار شما فقط بررسی منابع بیشتر نیست، بلکه باید به دنبال منابع مختلف باشید. اگر نمی‌توانید منابع معتبر مختلفی پیدا کنید که با منبعی که بررسی می‌کنید هماهنگ باشند، نباید آن منبع را باور کنید.

4. منابع خود را بررسی کنید.

حال زمان تمرین است. پرسشی در مورد چیزی که در کلاس به آن می‌پردازید یا چیزی که آنلاین دیده‌اید انتخاب کنید. منبعی را بیابید که پاسخ آن سوال را بدهد و در گروه‌های کوچک، از سوالات موجود در جزوه برای تصمیم‌گیری در مورد معتبر بودن منبع استفاده کنید.

اگر به ایده نیاز دارید، در ادامه چندین ایده برایتان تهیه کرده‌ایم.

• شما نیاز به ایده‌ای برای هدیه تولد دوست خود دارید. فروشگاه محلی در تبلیغات خود ادعا می‌کند ابزار جستجوی آنها، که شامل همان اجناس موجود در فروشگاه است، می‌تواند به شما کمک کرده تا برای هر کس در فهرست دوستان خود هدیه‌ای مناسب پیدا کنید. آیا چنین چیزی عملی است؟

• شما در حال خواندن نظرات افراد در مورد یک پیتزافروشی جدید هستید و متوجه می‌شوید که سه مورد از شش نظر ستاره‌دار از طرف افرادی است که نام خانوادگی آنها با نام خانوادگی صاحب رستوران یکی است. دو نفر دیگر نیز گفته‌اند بهترین پیتزای روی کره زمین را اینجا دارد و یک نفر هم گفته است که پیتزای آنجا نسبت به قیمتش بد نبوده است. همچنین چهارده نظر منفی وجود دارد. آیا نظرات مثبت شما را متقاعد می‌کند که پیتزای این پیتزافروشی را امتحان کنید؟

• یک تبلیغ پاپ‌آپ به شما می‌گوید بخشی از یک گروه بسیار کوچک هستید که برای امتحان «قرص پری دریایی» انتخاب شده‌اید که به شما قدرت نفس کشیدن در زیر آب را بدون وسایل غواصی می‌دهد. تنها کاری که باید انجام دهید این است که 9.99 دلار برای هزینه ارسال بفرستید. آیا شما آن را انجام می‌دهید؟

• شما خیلی از ویدیوهای وبلاگ‌نویس محبوب خود را تنها به این علت که خنده‌دار هستند، دوست دارید، اما در برخی از این ویدیوها چیزهای بدی در مورد اقلیت‌های گروهی گفته شده است که باعث ناراحتی شما شده است. آیا شما این ویدیوها را تنها به این دلیل که خنده‌دار و محبوب هستند می‌خرید؟ آیا فکر می‌کنید چنین ویدیوهایی روی مردم تأثیر بگذارند؟

نکته

سوالات دوستان ما هستند. وقتی سؤالات خوبی در مورد منابع و اطلاعاتی که ارائه می‌دهند بپرسید، اطلاعات بسیار بهتری به دست خواهید آورد. هرچه از منابع بیشتری استفاده کنید، بهتر است. به یاد داشته باشید که یک منبع عالی برای یک موضوع به این معنی نیست که آن منبع برای همه چیز عالی است.

تصمیم‌گیری در مورد موثق بودن منبع.

گام‌های مفید برای شناسایی منابع معتبر از منابع غیر معتبر.

مرحله 1

از عقل سلیم استفاده کنید

آیا چنین چیزی منطقی است؟

مرحله 2

سوالات خود را پرسید.

نه هر سوالی، بلکه این چهار سوال:

تجربه و تخصص

- آیا این منبع من را می‌شناسد یا به من اهمیت می‌دهد (و آیا این مهم است)؟
- آیا این منبع اطلاعات زیادی در مورد این موضوع دارد؟ آنها چگونه به این اطلاعات دست یافته‌اند؟

انگیزه

- این منبع از من می‌خواهد چه کار انجام دهم یا چه چیز را باور کنم و چرا آنها از من می‌خواهند کاری انجام دهم یا موضوعی را باور کنم؟
- اگر مردم این منبع را باور کنند به سود چه کسی و به ضرر چه کسی است؟

مرحله 3

تایید

آیا سایر منابع معتبر از گفته‌های این منبع پشتیبانی می‌کنند؟ از جستجوی آنلاین یا کار با متخصص رسانه‌ی مدرسه خود در کتابخانه به منظور یافتن سایر منابع اطلاعاتی در مورد موضوع مورد نظرتان استفاده کنید (منابع می‌توانند شامل کتاب یا اخبار یا مقالات مجله‌ها، چه به صورت آنلاین یا آفلاین باشند). مراحل 1 و 2 را نیز با آنها طی کرده و پرسش‌های مشابهی در مورد این منابع پرسید. اگر آنها همان اطلاعات را در مورد موضوع به شما بدهند، به احتمال زیاد آنها معتبر بودن منبع شما را تأیید می‌کنند.

مشاهده اطلاعات غیرقابل اعتماد در اینترنت

پیشینه سواد رسانه‌ای برای معلمان: پرسش‌های سواد رسانه‌ای و فنون مشاهده ابزارهایی هستند که دانش‌آموزان با استفاده از آنها راه خود را از میان انبوه اطلاعات نادرست، بدون هیچ مشکل یا وارد شدن آسیبی به روابطشان با دوستان یا خانواده، طی می‌کنند. اما آنها باید سؤال پرسند و به استفاده از پرس‌وجوی انتقادی اطلاعاتی که به دستشان می‌رسد، عادت کنند.

اهداف درس برای دانش‌آموزان



- ✓ **شناسایی** سرخ‌هایی که فریبنده بودن یک خبر یا منبع اطلاعاتی را نشان می‌دهند.
- ✓ **استفاده** از سوالات تحلیلی و فنون مشاهده دقیق برای ارزیابی اعتبار منبع.
- ✓ **درک** اهمیت بررسی اعتبار یک منبع قبل از به اشتراک گذاشتن آن.
- ✓ **عادت** کردن به به تجزیه و تحلیل تمامی اخبار و اطلاعات و نه فقط داستان‌هایی که به نظر مشکوک هستند.

برخی افراد یاد نمی‌گیرند چگونه اطلاعات جعلی را شناسایی کنند، و از این رو آنها را به اشتراک می‌گذارند. و این چنین است که این اطلاعات پخش می‌شوند و هنگامی که افراد بر اساس این اطلاعات نادرست درباره کارهایی که انجام می‌دهند یا به آن اعتقاد دارند، دست به انتخاب بزنند، شنیدن سخنان یکدیگر با حفظ آرامش، بحث کردن محترمانه، درک بهتر یکدیگر و حل مشکلات برای آنها بسیار سخت می‌شود.

از این رو اگر مطلبی شبیه اخبار باشد، چگونه می‌توانیم بین واقعی یا موثق بودن و جعلی یا گمراه کننده بودن آن تفاوت فائل شویم؟ سرخ‌هایی وجود دارد که بدان طریق می‌توانیم ترفندهایی که افراد بدان وسیله سعی در گمراه کردن ما دارند را تشخیص دهیم و سؤالاتی وجود دارند که می‌توانیم با طرح آنها داستان‌هایی که مبتنی بر واقعیت نیستند را تشخیص دهیم.

فعالیت



1. تفاوت این دو عکس در چیست؟

به تصویر زیر نگاهی بیندازید. با دقت نگاه کنید. آیا می‌توانید تفاوت بین این دو عکس را تشخیص دهید؟



• وسائل مورد نیاز:

• تصویر: «این عکس چه مشکلی دارد؟»

• دستورالعمل: «تصمیم‌گیری درمورد معتبر بودن یک موضوع» از درس 3 (صفحه 54)

• کاربرد: «تشخیص نشانی‌های اینترنتی جعلی»

پاسخ‌های کاربرد: «نشان دادن

آدرس‌های ساختگی»

واقعی:

abcnews.go.com

bbc.com/news

nbcnews.com

nytimes.com

washingtonpost.com

usatoday.com

ساختگی:

abcnews.com.co

abcnews-us.com

nbc.com.co

nytimesofficial.com

bbc1.site/business-news

washingtonpost.com

washingtonpost.com.co

usatoday.com

اگر کسی به شما بگوید کجا را نگاه کنید؛ چه؟ آیا این توصیه کار شما را آسان‌تر می‌کند؟

در این تصویر 9 تفاوت وجود دارد، آیا می‌توانید تمام آنها را مشخص کنید؟



تلاش برای تشخیص واقعی یا ساختگی بودن یک خبر شبیه به این بازی تصویری است. با نگاهی دقیق می‌توانید اطلاعات مهمی را به دست بیاورید و اگر بدانید به دنبال چه هستید، کار برایتان بسیار آسان‌تر خواهد شد.

بنابراین در اینجا چند سرنخ برای یافتن اطلاعات نادرست وجود دارد. اگر این موارد را مشاهده کردید، احتمالاً به یک داستان جعلی یا فریبنده نگاه می‌کنید.

یافتن URL جعلی

اولین بخشی که باید به آن نگاه کنید URL سایتی است که ماجرا را منتشر کرده است. برخی سایت‌های جعلی با انتخاب اسامی مشابه با یک سایت واقعی، اما با تفاوت‌های بسیار کوچک، سعی در فریب شما دارند. اکثر شرکت‌ها از URL کوتاه استفاده می‌کنند، زیرا به خاطر سپردن و نوشتن آن‌ها ساده‌تر است. بنابراین URL هایی با حروف اضافه و غیر ضروری اغلب سایت‌هایی حاوی اطلاعات نادرست هستند.

به جزوه نگاه کنید:

- دور تمام نشانی‌های اینترنتی که فکر می‌کنید واقعی هستند، خط بکشید.
- وقتی کار تمام شد، به کلیدپاسخ‌ها نگاه کنید. آیا تمام آنها را درست انتخاب کرده‌اید؟

از کجا می‌توان فهمید URL یک سایت خبری واقعی است یا ساختگی؟ یکی از راه‌ها جستجوی وبسایت سازمان خبری یا URL سازمان است. اگر سازمان معتبر باشد، کادری در سمت راست نتایج مشخص می‌شود که در آن بسیاری از پلتفرم‌ها با توضیحی درباره سازمان، از جمله آدرس وبسایت سازمان مشخص است. اگر URL معتبر نباشد، اغلب باید به سمت پایین صفحه رفته و عناوین مربوط به گزارش جعلی بودن سایت را ببینید و یا متوجه می‌شوید که سایت دیگر در دسترس نیست.

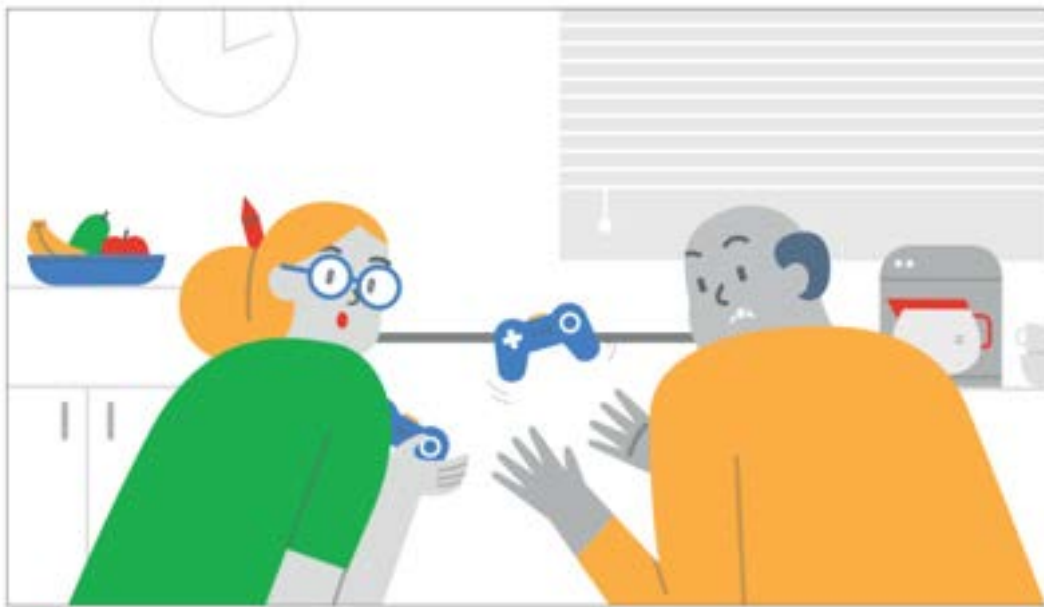
2. بازرسی سرفصل‌ها

گاهی اوقات شخصی خبری را بدون URL به اشتراک می‌گذارد. در چنین مواردی چند سرخ ساده به ما کمک خواهد کرد: الف) داستان اغلب با تصویری آغاز می‌شود که برای ما جالب است، مانند یک سگ زیبا، یک سلبریتی یا یک شیرین‌کاری غیر معمول. اما وقتی بر روی خبر کلیک می‌کنیم، داستان ربطی به عکس ندارد یا در کل چیز دیگری است.

ب) افرادی که به جای این که به شما اجازه دهند خود تصمیم بگیرید، سعی در متقاعد ساختن شما در همراهی با خود دارند اغلب از چیزهایی مانند حروف درشت، ALL CAPS، تاکید یا علامت تعجب استفاده می‌کنند تا شما را متقاعد سازند آنچه می‌بینید مهم است و روی آن کلیک کنید. چنین سایت‌هایی تله کلیک نامیده می‌شوند. روزنامه نگاران واقعی هرگز از این تکنیک‌ها استفاده نمی‌کنند.

ج) این سایت‌ها برای اینکه شما را وادار به خواندن داستانشان کنند از کلماتی مانند «تکان دهنده» یا «ظالمانه» یا «غافلگیرکننده» در عنوان خبر خود استفاده می‌کنند. آنها می‌دانند چنین کلماتی کنجکاوی ما را برمی‌انگیزد. اما روزنامه‌نگاران واقعی اجازه می‌دهند که اخبار خودش صحبت کند. آنها داستان را تعریف می‌کنند و به ما اجازه می‌دهند تصمیم بگیریم آیا این خبر تکان دهنده است یا غافلگیرکننده.

برای مثال به این تصویر و عنوان نگاه کنید:



بدون خواندن ماجرا تصور می‌کنید داستان از چه قرار است؟ چرا چنین فکر می‌کنید؟ چه مدرکی دارید؟

اما داستان از این قرار است:

نظرسنجی اخیر دانشگاه ایالتی از معلمان نشان داده است 86 درصد از معلمان همان کاری را انجام می‌دهند که همه بعد از آمدن از سرکار انجام می‌دهند. آنها کارهای شخصی خود را انجام داده، شام را درست می‌کنند، با خانواده وقت می‌گذرانند، کارهای خانه را انجام می‌دهند و برای روز بعد آماده میشوند. اما اخیراً بسیاری از معلمان کارهای غیرمنتظره‌ای انجام می‌دهند.

یک دهه پیش مشکلات اقتصادی باعث شد تا بسیاری ایالت‌ها بودجه آموزش و پرورش را کاهش دهند. این به معنای سال‌ها عدم افزایش حقوق معلمان بود. بسیاری از معلمان که قادر به تامین هزینه‌های اولیه با این حقوق ناچیز نبودند، اکنون به شغل دوم رو آورده‌اند. در برخی ایالت‌ها معلمان حتی برای افزایش حقوق دست به اعتصاب زدند تا بتوانند شغل دوم خود را رها کرده و زمان بیشتری را به دانش‌آموزان اختصاص دهند.

آیا داستان همان چیزی بود که فکر می‌کردید؟ به نظر شما عکس و عنوان درست بود یا گمراه کننده؟ مدرک شما چه بود؟

3. بازرسی منابع

سرنخ‌ها در تجزیه و تحلیل اخبار می‌توانند سودمند باشند، اما کافی نیستند. گاهی اوقات اخبار قابل اعتماد از تکنیک‌هایی برای جلب توجه ما استفاده می‌کنند و این تکنیک‌ها ممکن است جعلی به نظر برسند. گاهی اوقات منابع جعلی آنقدر در رونوشت کردن مطالب واقعی خوب عمل می‌کنند که به سختی می‌توان متوجه جعلی بودن آنها شد. تشخیص این دو از یکدیگر دشوار است. مثلاً...

به نظر شما موارد زیر سازمان‌های خبری موثقی هستند؟

اخبار آمریکا

نشنال ریویو

بازرس خبر

گزارش روزانه اخبار جهان

اخبار هفتگی جهان

NewsWatch33

در واقع فقط سازمان خبری نشنال ریویو واقعی است. چطور متوجه شدید؟ می‌توان کار را با جستجوی نام سازمان آغاز کرد. ببینید نام سازمان علاوه بر وبسایت خود سازمان دیگر در کجا ظاهر می‌شود. اگر این نام در ویکی پدیا یا مقاله‌ای از یک روزنامه یا سایت یک مجله خبری ظاهر شود، احتمالاً سازمانی معتبر است. و بعد ببینید آن مقالات در مورد آن سازمان چه می‌گویند! این امکان وجود دارد که همگی آنها خبر جعلی بودن سازمان را اعلام کرده باشند.

داستانی در مورد مدرسه، جامعه، آخرین مد، رژیم غذایی یا هر چیزی در اخبار مورد علاقه خود بیابید. برای تصمیم‌گیری در مورد واقعی یا دروغی بودن داستان، از سه مرحله در تصمیم‌گیری درباره آنچه معتبر است، همراه با سرنخ‌های جدیدی که می‌دانید، استفاده کنید.

مرحله 1: از عقل سلیم استفاده کنید.

پرسید: آیا چنین خبری منطقی است؟ آیا معقولانه است؟
گاهی اوقات جعلی بودن خبر بسیار واضح و مشخص است، به طور مثال اگر عنوان خبری مانند «سلبریتی‌ها از بیگانگان فضایی فرزندان نامشروع دارند» را جایی مشاهده کنید، منطقی به شما می‌گوید که چنین خبری جعلی و ساختگی است.
گاهی اوقات ساختگی بودن خبر چندان واضح نیست، در صورتی که:
الف) چیزی که می‌بینید با عقل جور در نمی‌آید.
ب) طبق تجربه می‌دانید که چنین چیزی درست نیست، یا
ج) با حقایقی که از قبل در ذهن دارید، هماهنگ نیست.
در این صورت شما به منبعی نگاه می‌کنید که احتمالا حاوی اخبار جعلی است.

مرحله 2: سوالات تخصص و انگیزه را مطرح کنید.

(به صفحات 52 و 53 مراجعه کنید)

مرحله 3: تایید

پرسید: آیا منابع معتبر دیگر از گفته‌های این منبع پشتیبانی می‌کنند؟
چه منابع دیگری این داستان را گزارش داده‌اند؟ (می‌توانید از جستجوی اینترنتی استفاده کنید تا ببینید آیا این داستان توسط سایر منابع خبری پوشش داده شده است یا خبر). این سایت شامل چه داستان‌های دیگری است؟ آنها همه از یک منظر هستند یا دیدگاه‌های زیادی در آنها گنجانده شده است؟ اگر نمی‌توانید دیگر انواع منابع موثقی که داستان را پوشش می‌دهند پیدا کنید، باید نسبت به آن منبع شک داشته باشید.

نکته

سوالات دوستان ما هستند. وقتی سؤالات خوبی در مورد منابع و اطلاعاتی که ارائه می‌دهند پرسید، اطلاعات بسیار بهتری به دست خواهید آورد. هرچه از منابع بیشتری استفاده کنید، بهتر است. به یاد داشته باشید که یک منبع عالی برای یک موضوع به این معنی نیست که آن منبع برای همه چیز عالی است.

تشخیص آدرس های اینترنتی جعلی

واقعی است یا تقلبی؟

دور جواب صحیح خط بکشید

usatoday.com	جعلی	واقعی
washingtonpost.com	جعلی	واقعی
abcnews-us.com	جعلی	واقعی
bbc.com/news	جعلی	واقعی
abcnews.go.com	جعلی	واقعی
nytimesofficial.com	جعلی	واقعی
nbc.com.co	جعلی	واقعی
washingtonpost.com	جعلی	واقعی
nytimes.com	جعلی	واقعی

در دام کلاهبردارها نیفتید: درس 5

اگر ما یک موتور جستجو بودیم.

بدون استفاده از هیچ‌گونه فناوری (در فعالیت بعدی این کار را انجام خواهیم داد)، دانش‌آموزان با یکدیگر «نتایج جستجو» را ایجاد کرده تا بر تمامی مراحل جستجوی اینترنتی اشراف کامل پیدا کنند.

ملاحظه: حاول أن تبقي باب المناقشة مفتوحا بحيث تم تصميم هذا النشاط لتشجيع التفكير النقدي، وليس لتقديم أي استنتاجات.

- ✓ آموزش اصول جستجوی آنلاین.
- ✓ جستجوی اطلاعات در مورد یک موضوع.
- ✓ آموختن چهار سوال اساسی برای ارزیابی اعتبار منبع.
- ✓ درک این موضوع که نتایج جستجو مجموعه‌ای از اطلاعات هستند، و نه صرفاً پاسخ به یک سوال.

اهداف درس برای دانش‌آموزان



جستجو چیست؟

اینترنت مکانی حاوی گزلیون‌ها (میلیاردها و میلیاردها) مورد اطلاعات است. جستجوی اینترنتی که گاهی موتور جستجو نیز نامیده می‌شود، به ما این امکان را می‌دهد تا این حجم عظیم دیوانه‌کننده اطلاعات که از سراسر جهان می‌آید را محدود سازیم. این یک نرم افزار است که افراد از آن به منظور یافتن اطلاعات در مورد انواع موضوعات استفاده می‌کنند.

ممکن است از این موضوع آگاهی داشته باشید که برای استفاده از این ابزار باید چند کلمه کلیدی در مورد موضوعی که می‌خواهید درباره آن اطلاعات بیشتری کسب کنید را در بخش نوار جستجو (بخش خالی در صفحه موتور جستجو) یا در پنجره مرورگر خود (جایی که آدرس وبسایت را تایپ می‌کنید) تایپ کنید. سپس دکمه «بازگشت» یا «جستجو» را فشار داده و به این ترتیب موتور جستجو جادوی خود را انجام می‌دهد (در حد نیم ثانیه)، و نتایج جستجوی خود را دریافت می‌کنید. البته چنین کاری جادو نیست. در جستجوی اینترنتی از الگوریتم استفاده می‌شود، به این صورت که افراد در شرکت جستجو به نرم‌افزار آموزش داده‌اند چگونه اطلاعات را برای شما پیدا کرده و نشان دهد. در حال حاضر نگران نحوه عملکرد الگوریتم‌ها نباشید. فقط باید بدانید که با جستجو به این نتایج رسیده‌اید.

در ضمن خوب است بدانید که نتایج جستجو لزوماً شامل پاسخ‌های یک سؤال نیستند. آنها فقط مجموعه اطلاعاتی هستند که شما به آنها علاقه دارید یا به دنبال آنها هستید. اگر سؤالی در موتور جستجو مطرح کنید، اغلب پاسخی را در نتایج جستجوی خود خواهید داشت، اما گاهی اوقات برای رسیدن به پاسخ مورد نظر به چندین جستجو نیاز است که به این کار «پالایش کردن» جستجو می‌گویند.

پس بیایید با تظاهر به این که یک موتور جستجو هستیم، نحوه عملکرد جستجو را تمرین کنیم:

1. دانش‌آموزان را به صورت گروه‌های 2 نفره سازماندهی کنید.

2. رونوشت برگه را بین هر دانش‌آموز توزیع کنید.

3. یک موضوع جستجو را با کلاس به اشتراک بگذارید. در ادامه چندین موضوع ارائه شده است:

- پیتزا
- طوفان
- هواپیما
- منظومه شمسی
- کشاورز
- فوتبال
- آتشفشان
- آشپزی
- کوسه
- ساخت و ساز
- دندانپزشک
- بسکتبال

فعالیت



4. **دانش‌آموزان با دوستان خود برای ایجاد «نتایج جستجوی» احتمالی در هر یک از دسته بندی‌های مندرج در جزوه شامل «وب‌سایت»، «تصویر»، «نقشه» و «ویدئو» کار کرده و نتایج آنها می‌تواند در قالب کلمات یا در صورت لزوم تصاویر نشان داده شود...**

دانش‌آموزان را تشویق کنید تا نوآور و خلاق باشند و مطمئن شوید هیچ پاسخ «اشتباهی» وجود ندارد. برای مثال اگر موضوع «کوسه» است، دانش‌آموزان ممکن است موارد زیر را بیان کند:

نتایج جستجو:

- وب‌سایت: اطلاعاتی در مورد انواع کوسه
- تصویر: نقاشی یک کوسه
- ویدئو: کوسه در اقیانوس شنا می‌کند.
- نقشه: موقعیت ساحلی که مردم در آن کوسه‌ای دیده‌اند.

5. **وقتی دانش‌آموزان هر چهار دسته‌بندی نتایج جستجو را برای موضوع داده شده به پایان رسانند، یکی را انتخاب کنید:** (وب‌سایت، تصویر، ویدئو یا نقشه) و در مورد آن صحبت کنید.

6. **از یکی از دانش‌آموزان در هر گروه بخواهید نمونه جستجوی خود را با کلاس به اشتراک بگذارد.**

به طور مثال فرض کنید موضوع «پیتزا» است. می‌توانید بخواهید هر گروه نتایج تصویری به دست آمده برای پیتزا را به اشتراک بگذارند. دانش‌آموزان می‌توانند نقاشی خود را بالا نگه داشته و در مورد آنچه خلق کرده‌اند، توضیح دهند. این کار به دانش‌آموزان اجازه می‌دهد تا تمام نتایج جستجوی مختلفی را که می‌توانند از یک جستجوی ساده به دست آورند، مشاهده کنند.

7. **پس از این که دانش‌آموزان مثال‌هایی را به اشتراک گذاشتند، سؤالات زیر را از کلاس بپرسید:**

- حدوداً چند نتیجه متفاوت داشتیم؟
- حدوداً چند نتیجه مشابه بودند؟
- اگر موضوع را به..... تغییر دهم، فکر می‌کنید نتایج چه تغییری خواهند کرد؟ به طور مثال اگر موضوع جستجو «پیتزا» باشد و بخواهم آن را به «پیتزای پیرونی» تغییر دهم، نتایج چه تغییری می‌کنند؟

پیشنهاد: هر 4 نوبت را تکمیل کنید.

- از هر نوبت یک موضوع متفاوت انتخاب کنید و همان مراحل گفته شده را تکرار کنید.
- هر 4 نوبت را تکمیل کنید تا بتوانید در مورد 4 نوع اصلی نتایج جستجو بحث کنید.

جستجوی اینترنتی ابزاری است که می‌توان برای یافتن اطلاعات آنلاین از آن استفاده کرد. اطلاعات ممکن است به شکل متن، فیلم، تصویر، نقشه و موارد دیگر باشند. کلمات کلیدی که در موتور جستجو تایپ می‌کنید تعیین‌کننده نتایجی هستند که به دست می‌آورد.

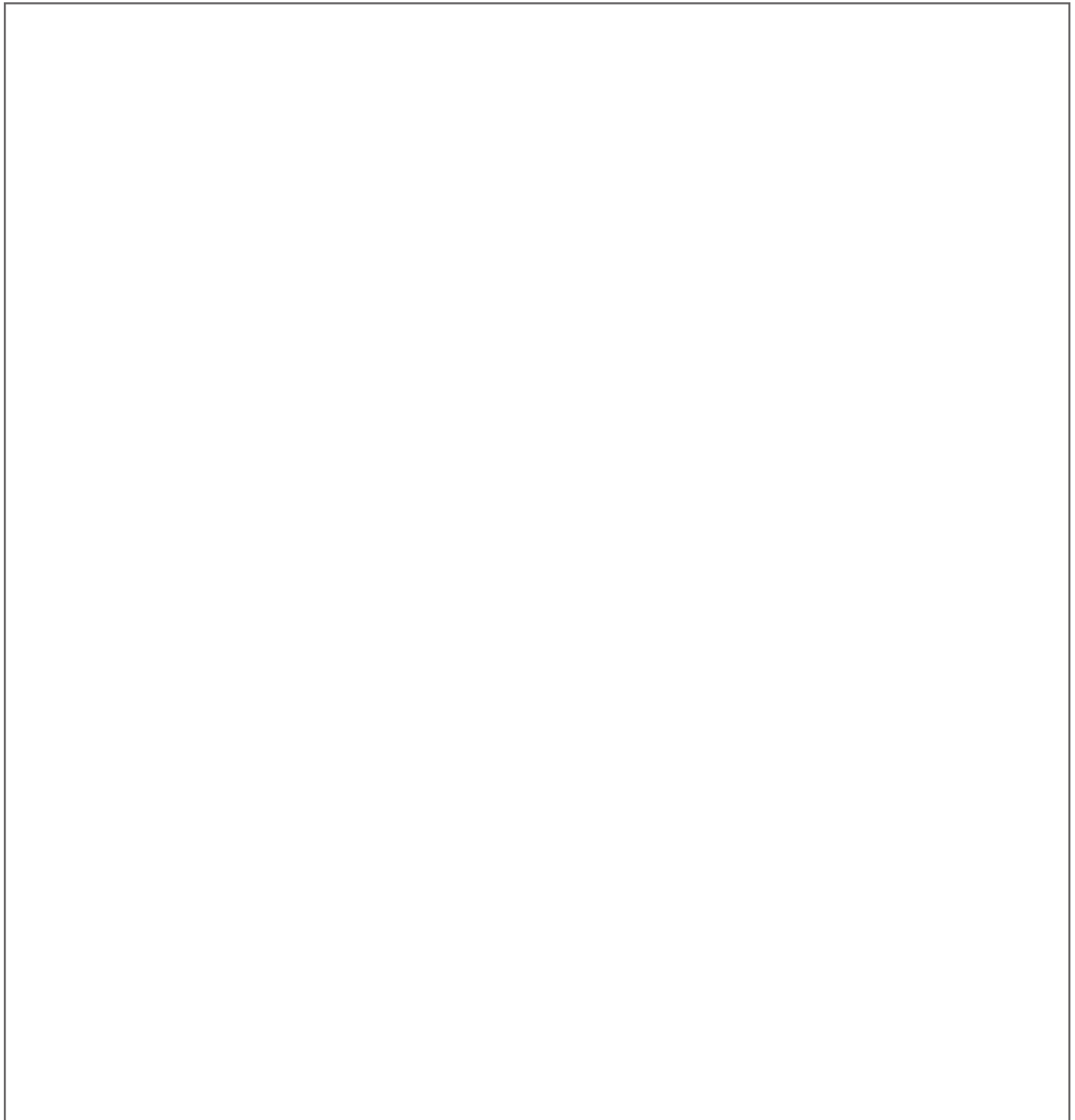
نکته

اگر یک موتور جستجو بودیم

وبسایت

موضوع جستجو

تصویر | ویدئو | نقشه



در دام کلاهبردارها نیفتید: درس 6

تمرین جستجوی اینترنتی

دانش‌آموزان با استفاده از موتور جستجو دست به کاوش در محیط آنلاین زده و نحوه ایجاد پرسش‌های مؤثرتر را تمرین می‌کنند.

اهداف درس برای دانش‌آموزان

- ✓ پیمایش موتور جستجو.
- ✓ تمرین جستجوی اطلاعات در مورد یک موضوع.
- ✓ ایجاد عبارت‌های جستجو.
- ✓ تغییر کلمات کلیدی و توجه به تفاوت نتایج.



بیابید حرف بزیم



جستجو ابزاری است که به شما کمک می‌کند اطلاعات را در اینترنت پیدا کنید. برای استفاده از جستجو می‌توانید به یک موتور جستجو رفته و یک سوال یا کلمات کلیدی را در نوار جستجو تایپ کنید تا اطلاعاتی در مورد موضوعی که می‌خواهید درباره آن بیشتر بدانید به دست آورید. گاهی اوقات استفاده از کلمات کلیدی بهتر از پرسیدن سوال است. به این دلیل که اولاً کلماتی که در جستار خود استفاده می‌کنید و دوماً ترتیبی که آنها را قرار می‌دهید واقعا مهم هستند. اگر فقط سؤالی بپرسید، ممکن است کلمات و ترتیبی که به موتور جستجو کمک می‌کند نتایج مورد نظر شما را نشان دهد، وجود نداشته باشد. اما هیچ جای نگرانی نیست، اگر دوست دارید کارتان را با طرح یک سوال شروع کنید هم اشکالی ندارد.

نکته مهم شروع کردن است، زیرا اغلب اوقات برای دستیابی به اطلاعاتی که به دنبال آن هستید به بیش از یک پرس‌وجو نیاز است. بنابراین سوال خود را در موتور جستجو تایپ کنید، به نتایج جستجو نگاه کنید و اگر نتایج به اندازه کافی خوب نبودند، می‌توانید از این نتایج برای راهنمایی گرفتن در مورد چگونگی ایجاد یک پرسش بهتر و حتی نزدیک‌تر شدن به آنچه دنبالش هستید، استفاده کنید.

به عنوان مثال: می‌خواهم یک باغچه داشته باشم. می‌خواهم سبزیجاتی بکارم که بتوانم از آنها در پخت و پز استفاده کنم.

- نمی‌دانم چطور این کار را انجام دهم، بنابراین در اینترنت جستجو کرده تا بفهمم چگونه این کار را در حیاط منزل خود انجام دهم.
- در موتور جستجو این سوال را تایپ می‌کنم که «چگونه یک باغچه داشته باشیم؟».
- صفحه رایانه خود را نمایش دهید تا دانش‌آموزان بتوانند شما را در حال جستجو ببینند.
- بسیار خوب، بیابید به نتایج نگاهی بیندازیم.

نتایج را با کلاس بررسی کنید. حتماً به این نکته اشاره کنید که وبسایت‌ها، تصاویر، ویدیوها و انواع دیگری از نتایج نیز وجود دارد. همچنین به نتایجی که در مورد باغ سبزیجات و استفاده از آنها در پخت و پز اشاره‌ای ندارند نیز اشاره کنید.

- متوجه شدم که بسیاری نتایج به دست آمده در مورد انواع باغچه‌ها هستند، اما من به اطلاعاتی در مورد ایجاد یک باغچه در خانه و در حیاط خود نیاز دارم. همچنین می‌خواهم سبزیجاتی پرورش دهم که بتوانم در پخت و پز از آنها استفاده کنم. احتمالاً باید یک کلمه کلیدی در مورد سبزیجات اضافه کنم، درست است؟ خوب، بیابید باز آن را جستجو کنیم: «سبزیجات باغچه خانگی»
- صفحه رایانه خود را نمایش دهید تا دانش‌آموزان بتوانند شما را در حال جستجو ببینند.
- به این نتایج نگاهی بیندازید. متوجه چه شدید؟

به دانش‌آموزان اجازه دهید آنچه را که در نتایج جستجو مشاهده می‌کنند با یکدیگر به اشتراک بگذارند

هر دو مجموعه نتایج جستجو به من اطلاعاتی در مورد راه اندازی یک باغچه دادند، درست است؟ اما مجموعه اطلاعات اول درباره انواع باغچه بود. من فهمیدم که باید چند کلمه کلیدی مهم دیگر را به درخواست اصلی خود اضافه کنم تا نتایج جستجوی مورد نیاز برای یادگیری نحوه راه اندازی یک باغچه برای آشپزی را به دست بیاورم (در هر صورت، آیا می‌دانستید که به آن «باغچه آشپزخانه‌ای» می‌گویند؟)

جستجو ابزاری است که به شما کمک می‌کند اطلاعات را در اینترنت پیدا کنید. برای استفاده از جستجو می‌توانید به یک موتور جستجو رفته و یک سوال یا کلمات کلیدی را در نوار جستجو تایپ کنید تا اطلاعاتی در مورد موضوعی که می‌خواهید درباره آن بیشتر بدانید به دست آورید. گاهی اوقات استفاده از کلمات کلیدی بهتر از پرسیدن سوال است. به این دلیل که اولاً کلماتی که در جستار خود استفاده می‌کنید و دوماً ترتیبی که آنها را قرار می‌دهید واقعا مهم هستند. اگر فقط سوالی بپرسید، ممکن است کلمات و ترتیبی که به موتور جستجو کمک می‌کند نتایج مورد نظر شما را نشان دهد، وجود نداشته باشد. اما هیچ جای نگرانی نیست، اگر دوست دارید کارتان را با طرح یک سوال شروع کنید هم اشکالی ندارد.

نکته مهم شروع کردن است، زیرا اغلب اوقات برای دستیابی به اطلاعاتی که به دنبال آن هستید به بیش از یک پرس‌وجو نیاز است. بنابراین سوال خود را در موتور جستجو تایپ کنید، به نتایج جستجو نگاه کنید و اگر نتایج به اندازه کافی خوب نبودند، می‌توانید از این نتایج برای راهنمایی گرفتن در مورد چگونگی ایجاد یک پرسش بهتر و حتی نزدیک‌تر شدن به آنچه دنبالش هستید، استفاده کنید.

به عنوان مثال: می‌خواهم یک باغچه داشته باشم. می‌خواهم سبزیجاتی بکارم که بتوانم از آنها در پخت و پز استفاده کنم.

- نمی‌دانم چطور این کار را انجام دهم، بنابراین در اینترنت جستجو کرده تا بفهمم چگونه این کار را در حیاط منزل خود انجام دهم.
 - در موتور جستجو این سوال را تایپ می‌کنم که «چگونه یک باغچه داشته باشم؟».
 - صفحه رایانه خود را نمایش دهید تا دانش‌آموزان بتوانند شما را در حال جستجو ببینند.
 - بسیار خوب، بیایید به نتایج نگاهی بیندازیم.
- نتایج را با کلاس بررسی کنید. حتماً به این نکته اشاره کنید که وب‌سایت‌ها، تصاویر، ویدیوها و انواع دیگری از نتایج نیز وجود دارد. همچنین به نتایجی که در مورد باغ سبزیجات و استفاده از آنها در پخت و پز اشاره‌ای ندارند نیز اشاره کنید.
- متوجه شدم که بسیاری نتایج به دست آمده در مورد انواع باغچه‌ها هستند، اما من به اطلاعاتی در مورد ایجاد یک باغچه در خانه و در حیاط خود نیاز دارم. همچنین می‌خواهم سبزیجاتی پرورش دهم که بتوانم در پخت و پز از آنها استفاده کنم. احتمالاً باید یک کلمه کلیدی در مورد سبزیجات اضافه کنم، درست است؟ خوب، بیایید باز آن را جستجو کنیم: «سبزیجات باغچه خانگی»
- صفحه رایانه خود را نمایش دهید تا دانش‌آموزان بتوانند شما را در حال جستجو ببینند.
- به این نتایج نگاهی بیندازید. متوجه چه شدید؟

به دانش‌آموزان اجازه دهید آنچه را که در نتایج جستجو مشاهده می‌کنند با یکدیگر به اشتراک بگذارند

هر دو مجموعه نتایج جستجو به من اطلاعاتی در مورد راه اندازی یک باغچه دادند، درست است؟ اما مجموعه اطلاعات اول درباره انواع باغچه بود. من فهمیدم که باید چند کلمه کلیدی مهم دیگر را به درخواست اصلی خود اضافه کنم تا نتایج جستجوی مورد نیاز برای یادگیری نحوه راه اندازی یک باغچه برای آشپزی را به دست بیاورم (در هر صورت، آیا می‌دانستید که به آن «باغچه آشپزخانه‌ای» می‌گویند؟)

هرچه بیشتر ایجاد عبارت‌های جستجو را تمرین کنید، جستجو برایتان آسان‌تر می‌شود. شما همواره می‌توانید با یک سوال کار خود را شروع کنید، و اگر پاسخ خود را دریافت نکردید، نتایج جستجو کلمات کلیدی را در اختیار شما قرار می‌دهد که می‌توانید با استفاده از آنها سعی کنید به آنچه که باید بدانید نزدیکتر شوید. اگر می‌خواهید با کلمات کلیدی شروع کنید و مطمئن نیستید که چه کلماتی استفاده کنید، فقط باید بدانید که هیچ کلمه کلیدی اشتباهی وجود ندارد. فقط امتحان کنید! اگر نتایجی که انتظارش را داشتید، نمی‌بینید، همیشه می‌توانید یک پرسش متفاوت را امتحان کنید. بیایید امتحان کنیم.

فعالیت



• وسایل مورد نیاز:

- کاربرگ: «تمرین جستجوی اینترنتی» (یکی برای هر دانش‌آموز)
- دستگاه متصل به اینترنت

1. اولین عبارت جستجو را ایجاد کنید.

به دانش‌آموزان توضیح دهید قصد دارید با استفاده از موتور جستجو دست به کاوش زده و ایجاد عبارت‌های جستجو را تمرین کنند در جزوه آنها چهار شخصیت مختلف را پیدا می‌کنند که هر شخصیت (در یک حباب فکری) به چیزی فکر می‌کند که می‌خواهند درباره آن بیشتر بیاموزند. سپس از دانش‌آموزان بخواهید...

- عبارت جستجوی اصلی (ارائه شده در جزوه) را در موتور جستجو تایپ کنید و نتایج جستجو را بررسی کنند.
- 4 تا 5 نتیجه به دست آمده را در دفترچه یادداشت خود یادداشت کنند.

2. پرسش جستجوی (دوم) خود را ایجاد کنید.

از دانش‌آموزان بخواهید دوباره به آنچه شخصیت می‌خواهد بداند (در حباب فکر) نگاه کنند. از دانش‌آموزان بپرسید آیا نتایج جستجوی اصلی اطلاعات کافی مرتبط با این موضوع را ارائه می‌دهد؟

- دانش‌آموزان را هدایت کنید تا درخواست اصلی را طوری تغییر دهند که شامل کلمات کلیدی شده و نتایج جستجوی مفیدتری برای آنها به ارمغان آورد.

نکته: دانش‌آموزان می‌توانند کلمات کلیدی را که در اولین نتایج جستجو یا در حباب فکر شخصیت پیدا کرده‌اند، جستجو کنند. از آنها بخواهید که این عبارت جستجوی دوم را در موتور جستجو تایپ کنند و نتایج جستجو را بررسی کنند.

- از دانش‌آموزان بخواهید 4-5 نتیجه را در جزوه خود ثبت کنند.

2. پرسش جستجوی (دوم) خود را ایجاد کنید.

از دانش‌آموزان بخواهید شریکی پیدا کنند و نحوه تغییر عبارت جستجوی اصلی و انواع نتایجی که از آن عبارت جستجوی اصلاح‌شده به دست آورده‌اند را با شرکای خود در میان بگذارند. از آنها بخواهید آنچه را که در یک بحث کوتاه کلاسی کشف کرده‌اند را به اشتراک بگذارند.

4. مراحل 1-3 را برای بخش‌های باقی مانده تکرار کنید.

هر چه بیشتر ایجاد پرسش‌های جستجو را بیشتر تمرین کنید، پیدا کردن اطلاعات مورد نظر در موتور جستجو آسان‌تر خواهد شد.

نکته

تمرین جستجوی اینترنتی

عبارت جستجوی اصلی

هایی در مورد شخصیت‌های خیالی و رمز و راز کتاب

نتایج جستجو

درخواست جستجوی اصلاح شده

نتایج جستجو -

عبارت جستجوی اصلی

کیک میوه بدون شکلات

نتایج جستجو

پرس و جوی جستجوی اصلاح شده -

نتایج جستجو

به دنبال کتابی برای خواندن هستم. عاشق موضوعات اسرارآمیز هستم! همچنین از خواندن کتاب‌هایی که شخصیت‌های خیالی دارند برم. فکر می‌کنم معلم من چنین‌که در آینده زندگی می‌کنند لذت می‌هایی را علمی تخیلی می‌نامد کتاب.



می‌خواهم برای تولد خواهرم کیک درست کنم. او شکلات دوست دانم چه کیک می‌توانم‌آید. نمی‌دارد، اما از میوه خوشش می‌درست کنم.



تمرین جستجوی اینترنتی

- عبارت جستجوی اصلی
- مشاغل بازی های ویدیویی
- نتایج جستجو

جستجوی بازبینی شده -

- نتایج جستجو

- عبارت جستجوی اصلی
- برای ماهیگیری به چه چیزهایی نیاز دارم؟
- نتایج جستجو

جستجوی بازبینی شده -

- نتایج جستجو

های ویدیویی هستم عاشق بازی فکر می‌کنم اگر بزرگ شوم و در یک شرکت بازی‌های ویدئویی کار کنم چه عالی خواهد شد... اگر روزی چنین کاری داشته شود باشم خیلی باحال می



پسر عمویم از من دعوت کرده است با او به ماهیگیری بروم. من قبلاً هرگز ماهیگیری نکرده‌ام، بنابراین نمی‌دانم چه نوع تجهیزاتی باید با خود بیاورم.



به دام کلاهبردارها نیفتید: درس 7 اینترنت: رودخانه واقعیت

رودخانه‌ای که از اینترنت می‌گذرد و جریان آن واقعیت و مجاز است. اما همه چیز آنطور که به نظر می‌رسد، نیست. برای عبور از گذر تند آب باید بهترین قضاوت خود را به کار ببرید و گرفتار دزدان هویت (فیشر) که در این آب‌ها کمین کرده‌اند، نشوید. یک مرورگر وب را روی دسکتاپ یا دستگاه تلفن همراه خود (به عنوان مثال تبلت) باز کنید و به g.co/RealityRiver بروید.

موضوعات مورد بحث

- از دانش‌آموزان بخواهید بازی رودخانه واقعیت را بازی کنند و از سؤالات زیر به منظور گفتگوی بیشتر در مورد درس‌های آموخته شده در بازی استفاده کنند. اکثر دانش‌آموزان با انفرادی بازی کردن بیشترین بهره را از این تجربه می‌برند، اما شما می‌توانید از آنها بخواهید بازی را به صورت گروهی نیز انجام دهند. این کار ممکن است برای دانش‌آموزان کم سن و سال‌تر بهتر باشد.
- زمانی را توصیف کنید که باید تصمیم می‌گرفتید چیزی واقعی است یا جعلی. متوجه چه علائمی شدید؟
- فیشر چه کسی است؟ رفتارهای این افراد و چگونگی تأثیر آن‌ها بر بازی را شرح دهید.
- آیا بازی رودخانه واقعیت شیوه ارزیابی شما از موضوعات و افراد آنلاین را در آینده تغییر داده است؟ اگر چنین است، چگونه؟
- فکر می‌کنید پس از شرکت در این درس و انجام بازی، در چه زمینه‌ای متفاوت عمل خواهید کرد؟
- چه سرنخ‌هایی وجود دارد که نشان می‌دهند خطری «خاموش» یا وحشتناک در یک موقعیت خاص آنلاین وجود دارد؟
- وقتی به چیزی مشکوک در اینترنت برخورد می‌کنید چه احساسی دارید؟
- اگر در مورد حقیقی بودن چیزی مطمئن نیستید، چه کاری باید انجام دهید؟





در حفظ اسرار خود کوشا باشید.

در حفظ اسرار خود کوشا باشید.

کلاس‌های 2-6	درس 1 این که من نبودم!	نمای کلی درس
کلاس‌های 2-6	درس 2 چگونه یک رمز عبور عالی بسازیم.	
کلاس‌های 2-6	درس 3 آن را برای خود نگه دارید	
کلاس‌های 2-6	درس 4 اینترنتند: برج گنج	
<p>هر فردی که از یک دستگاه متصل به اینترنت مانند دستگاه بازی دیجیتالی، تلفن، دستیار دیجیتالی، رایانه و غیره استفاده می‌کند باید از اصول اولیه حفظ حریم خصوصی و امنیت آنلاین آگاه باشد. محافظت از این دستگاه‌ها و اطلاعات شخصی درون آنها که می‌تواند اطلاعاتی در مورد خودتان، خانواده و دوستانتان باشد به این معنی است که باید در مورد مطالب ورودی و خروجی دقت عمل به خرج دهید و در مورد رمزهای عبور هوشمندانه عمل کنید.</p>		موضوعها:
<ul style="list-style-type: none">✓ یاد می‌گیرند که چرا حریم خصوصی و امنیت مهم است و چه ارتباطی با یکدیگر دارند.✓ نحوه ایجاد رمزهای عبور قوی و نگه داشتن آنها نزد خود (و بزرگسالانی که به آنها اطمینان دارند) را تمرین می‌کنند.✓ ابزارها و تنظیماتی که در برابر کلاهبرداری‌ها، هکرها و سایر تهدیدات از آنها محافظت می‌کنند را بررسی کنند.		اهداف درس برای دانش‌آموز:
<p>استانداردهای ISTE برای مربیان: 1a, 2c, 3b, 3c, 3d, 4b, 6a, 6d, 7a</p> <p>استانداردهای ISTE برای دانش‌آموزان 2016: 1c, 1d, 2b, 2d, 3d, 6a</p> <p>AASL استانداردهای یادگیری: I.a.1, I.c.3, II.c.1, III.a.2, III.b.1, III.c.1, III.d.1, III.d.2, IV.b.3, V.d.3, VI.a.1, VI.d.1</p>		استانداردهای در نظر گرفته شده

اما این که من نبودم!

دانش‌آموزان نتایج به اشتراک گذاری رمز عبور خود و تأثیری که این اقدامات ممکن است داشته باشند را بررسی می‌کنند.

- ✓ آموزش این که اشتراک‌گذاری رمز عبور به دیگران امکان کنترل ردپای دیجیتالی شما را به دیگران می‌دهد.
- ✓ در نظر گرفتن این که وقتی شخصی با جعل هویت وارد سیستم شما می‌شود چه اتفاقی ممکن است رخ دهد.
- ✓ دانستن این که چگونه اقدامات شخص دیگری می‌تواند بر روی ردپای دیجیتال شما و شما تاثیر بگذارد!

اهداف درس برای دانش‌آموزان للطلاب:



وقتی رمز عبور یا گذرواژه خود را به اشتراک می‌گذارید چه اتفاقی می‌افتد؟

به گذرواژه‌ای فکر کنید که برای برنامه یا دستگاه خود ایجاد کرده‌اید. شاید این گذرواژه برای باز کردن قفل تلفن همراه یا ورود به بازی یا برنامه ویدیویی مورد علاقه‌تان به کار برده شود. آیا تا به حال گذرواژه خود را با دیگران به اشتراک گذاشته‌اید؟ خوب، بیایید با هم صادق باشیم، بسیاری از ما این کار را کرده‌ایم، اما دلیل مهمی وجود دارد که چرا نباید گذرواژه خود را به اشتراک بگذاریم.

شما چیزی به نام ردپای دیجیتال دارید. ردپای دیجیتال تمام کارهای شما در دنیای آنلاین را نشان می‌دهد. هرچه در اینترنت به اشتراک می‌گذارید مانند لایک‌ها، نظرات، نام صفحه نمایش، عکس‌ها، پیام‌ها، موارد ضبط شده، و غیره شامل این ردپا می‌شوند و از این طریق دیگران در مورد شما و علایق شما چیزهایی می‌فهمند. این ردپا بر شهرت و خوشنامی شما و این که دیگران در مورد شما چه فکری می‌کنند نیز تأثیر می‌گذارد. مردم بر اساس ردپایی که از خود به جا می‌گذارید، در مورد شما حدس‌هایی زده یا فرضیاتی ارائه می‌دهند. این نکته‌ای است که هنگام آنلاین بودن باید از آن آگاه باشید.

بیایید حرف بزنیم



نکته مهم دیگر این است که وقتی گذرواژه خود را به اشتراک می‌گذارید، کنترل ردپای دیجیتال خود را به شخص دیگری واگذار کرده و در واقع به آنها اجازه می‌دهید به ایجاد این ردپا کمک کرده و طرز فکر دیگران را در مورد شما را شکل دهند. بله، درست است! از آنجایی که این رد پای شماست، همه بر این باورند که شما هستید که آن را ایجاد کرده‌اید. بنابراین اگر شخصی با رمز عبور شما کاری انجام دهد که دوست ندارید، مردم فکر می‌کنند که شما این کار را انجام داده‌اید! به همین دلیل بسیار مهم است که رمزهای عبور خود را در اختیار دیگران قرار ندهید.

به عنوان مثال: فرض کنید رمز عبور رسانه اجتماعی خود را با دوستی به اشتراک گذاشته‌اید. دوست شما به جای شما وارد سیستم شده و برای یکی از همکلاسی‌های شما این پیام را ارسال می‌کند: «می‌توانی پاسخ تکالیف امروز را برایم ارسال کنی؟». روز بعد همکلاسی شما نزد معلم رفته و می‌گوید شما از او خواسته‌اید تکالیفش را برایتان بفرستد و در واقع در انجام تکالیف خود تقلب کرده‌اید. سپس پیامی که دوستان از حساب شما فرستاده است را به معلم نشان می‌دهد. فکر می‌کنید معلم حرف چه کسی را باور خواهد کرد؟ این موضوع چه تأثیری بر شهرت شما خواهد داشت؟ چه اتفاقی ممکن است بیفتد؟

در مورد نتایج احتمالی ایده‌پردازی کنید. مثلاً: معلم با والدین شما تماس می‌گیرد. نمرهٔ این درس را از دست می‌دهید. ردپای دیجیتالی شما نشان می‌دهد شما سعی داشتید در مدرسه تقلب کنید. شما با دوستان که این پیام را فرستاده است دعوا می‌کنید.

به یاد داشته باشید ردپای دیجیتالی شما همان خودتان در دنیای آنلاین هستید. هر زمان که رمز عبور خود را با شخصی به اشتراک می‌گذارید، کنترل ردپای دیجیتالی خود را به او داده‌اید و این کار می‌تواند بر نگرش دیگران در مورد شما، چه در دنیای اینترنت و چه هر جای دیگر، تأثیر بگذارد. بیایید این ایده را با یکدیگر بررسی کنیم.

1. به دانش‌آموزان کمک کنید با یکدیگر گروه دوفره تشکیل دهند.
2. یک حساب کاربری انتخاب کنید.

دانش‌آموزان انتخاب می‌کنند.

که برای چه نوع حسابی رمز عبور خود را به اشتراک بگذارند و آن را در بالای کاربرگ می‌نویسند: حساب رسانه‌های اجتماعی، حساب بازی، تلفن، تبلت/رایانه یا سرویس پخش.

3. یک اقدام را انتخاب کنید.

شرکا اولین کادر را یکی از گزینه‌های زیر پر کرده و یا خود در این مورد فکر می‌کنند. این اقدام توسط شخصی انجام می‌شود که رمز عبور دیگری را دریافت کرده است. آنها می‌توانند آنچه را که به ذهنشان می‌رسد را ترسیم کرده یا بنویسند یا از میان اقدامات ممکن یکی را انتخاب کنند:

- «لایک» تمام پست‌های اخیر فرد مورد علاقه شما.
- خرید یک لباس 100 دلاری.
- ارسال پیامی مانند، «به نظرت کارمن خیلی روی مخ نیست.»
- بازی مورد علاقه شما را انجام می‌دهد، اما امتیاز از دست می‌دهد.
- برنامه‌های جدید را دانلود می‌کند.
- تصویر مستهجنی را در صفحه شبکه‌های اجتماعی شما به اشتراک می‌گذارد.
- همه نوشته‌های شما را می‌خواند و با شخص دیگری به اشتراک می‌گذارد.
- قسمت‌های یک برنامه نامناسب را تماشا می‌کند.

4. نتیجه‌گیری

در کادر دوم دانش‌آموزان نتیجه احتمالی اقدام انتخابی را می‌نویسند.

فعالیت



وسائل مورد نیاز:

- کاربرگ: «اما این که من نبودم!» (یکی برای هر گروه دو نفره)

5. گفتگو

- در کلاس از چند دانش‌آموز بخواهید اقدامات و نتایج به دست آمده را با دیگران به اشتراک بگذارند. در زیر چند سؤال وجود دارد که می‌توانید پس از به اشتراک‌گذاری از گروه‌ها بپرسید:
- چرا آن عمل را انتخاب کردید (یا ایجاد کردید)؟
 - چگونه در مورد نتیجه تصمیم گرفتید؟
 - اگر می‌دانستید نتیجه این کار چنین است، چه تغییری در اقدامات خود ایجاد می‌کردید؟

6. ردپای دیجیتال

در کادر آخر دانش‌آموزان در مورد این که چگونه این عمل و نتیجه بر احساسات، زندگی یا ردپای دیجیتالی تأثیر می‌گذارد جمله‌ای می‌نویسند. هر چه که می‌خواهد باشد. دانش‌آموزان را راهنمایی کنید تا در این مورد بیندیشند که چگونه این کار بر شهرت آنها تأثیر گذارده و یا با این کار در نظر دیگران چگونه جلوه خواهند کرد. از داوطلبان یا افراد گروه بخواهید درباره آنچه نوشته‌اند و در مورد دیدگاه خود در زمینه داستانی که خلق کرده‌اند، بحث کنند.

نکته:

وقتی رمز عبور خود را به اشتراک می‌گذارید، کنترل ردپای دیجیتال خود را به شخص دیگری واگذار می‌کنید، اما با این این شما هستید که در قبال هر کاری که آن فرد با رمز عبور شما انجام می‌دهد، پاسخگو هستید. اگر می‌خواهید در دیدگاه دیگران بد نشوید همیشه کنترل گذرواژه‌های خود را در اختیار داشته باشید و آنها را با هیچ‌کس به جز والدین یا بزرگسال دیگری که کاملاً به آنها اعتماد دارید، به اشتراک نگذارید.

اما این که من نبودم!

تبلت/رایانه
 تلفن

حساب رسانه اجتماعی
 سرویس پخش فیلم

من رمز عبور: را به اشتراک گذاشتم:
 حساب بازی

اقدام

تبعات

تأثیر رد پای دیجیتال

چگونه یک گذرواژه عالی بسازیم.

دانش‌آموزان یاد می‌گیرند چگونه یک گذرواژه کامل بسازند و همچنین چگونه مطمئن شوند که این گذر واژه خصوصی باقی خواهد ماند

اهداف درس برای دانش‌آموزان



- ✓ درک اهمیت عدم به اشتراک گذاری گذرواژه‌ها، به جز با والدین یا سرپرست.
- ✓ درک اهمیت قفل صفحه نمایش که از دستگاه‌ها محافظت می‌کنند.
- ✓ آموختن نحوه ایجاد گذرواژه‌هایی که حدس زدن آنها دشوار است، اما به خاطر سپردن آنها آسان است.
- ✓ انتخاب شیوه‌های ایمن و مناسب برای تنظیمات ورود به سیستم، از جمله تأیید دو مرحله‌ای .

بیایید حرف بزنیم



کار از محکم کاری عیب نمی‌کند.

فناوری دیجیتال ارتباط ما را با دوستان، همکلاسی‌ها، معلمان و خویشاوندان را آسان می‌کند. ما می‌توانیم به روش‌های مختلف با این افراد ارتباط برقرار کنیم: روش‌هایی مانند ارسال پیام، بازی کردن و ارسال محتوا هایی مانند متن، عکس و فیلم و با استفاده از تلفن، تبلت، لپ‌تاپ و دستیار دیجیتال. (چگونه با دوستان خود ارتباط برقرار می‌کنید؟)

اما همین ابزارهایی که اشتراک‌گذاری اطلاعات را برای ما آسان کرده‌اند، می‌توانند سرقت این اطلاعات و استفاده از آنها را برای آسیب رساندن به دستگاه‌های ما، سرقت هویت ما یا آسیب رساندن به روابط و شهرت ما را برای هکرها و کلاهبرداران آسان کنند.

محافظت از خود، اطلاعات و دستگاه‌هایمان به معنای انجام کارهایی ساده و هوشمندانه مانند استفاده از قفل صفحه تلفن، دقت در زمان ارسال اطلاعات شخصی در دستگاه‌هایی که قفلشان باز است یا توسط افراد زیادی (مانند مدرسه) استفاده می‌شود و مهم‌تر از همه، ایجاد گذرواژه‌های قوی و به اشتراک نگذاشتن آنها است.

چه کسی می‌تواند حدس بزند که دو رمز عبور رایج کدام هستند؟ (پاسخ: «123456» و «password»)

Who can guess what the two most commonly used passwords are? (Answer: "1 2 3 4 •

"6 5" and "password")

• بیایید دیگر گذرواژه‌های نامناسب و آنچه که آنها را به طور خاص نامناسب می‌کنند را بررسی کنیم. (مثال: نام کامل شما، شماره تلفن شما، کلمه «شکلات»، نام سگ شما، آدرس شما و از این قبیل.»

چه کسی فکر می‌کند این گذرواژه‌ها خوب و مناسب هستند؟

فعالیت



وسائل مورد نیاز:

- دستگاه‌های متصل به اینترنت
- وایت بورد یا صفحه نمایش
- جزوه: «راهنمای ایجاد گذرواژه‌های کامل»

در ادامه ایده‌های به منظور ایجاد یک گذرواژه بسیار امن ارائه شده است:

- به یک عبارت سرگرم کننده فکر کنید که بتوانید آن را به خاطر بسپارید. این عبارت می‌تواند متن آهنگ مورد علاقه شما، عنوان کتاب، یک جمله در یک فیلم و از این قبیل باشد.
- از هر کلمه در عبارت، حرف اول یا دو حرف اول را انتخاب کنید.
- برخی از حروف را به نمادها یا اعداد تغییر دهید.
- برخی از حروف را بزرگ و برخی را کوچک کنید.

بیاپید مهارت‌های جدید خود را با بازی گذرواژه تمرین کنیم.

1. گذرواژه ایجاد کنید.

به تیم‌های دو نفره تقسیم شوید. هر تیم 60 ثانیه وقت دارد تا یک گذرواژه درست کند.

گزینه چالش برانگیز: دانش‌آموزان ابتدا سرخ‌هایی را با کلاس به اشتراک می‌گذارند تا ببینند کلاس به چه مقدار اطلاعات

زمینه‌ای نیاز دارد تا بتواند حدس درستی بزند.

2. گذرواژه‌ها را مقایسه کنید.

دو گروه گذرواژه خود را همزمان روی تابلو می‌نویسند.

3. رای دهید!

برای هر جفت گذرواژه همه کلاس رای داده و سپس به بحث در این خصوص خواهند پرداخت که کدام یک از آنها قوی‌تر است.

ایجاد گذرواژه‌های قوی کاری مهم و سرگرم کننده است.

نکته:

دستورالعمل‌هایی برای ایجاد گذرواژه‌های قوی

در ادامه به ارائه نکاتی برای ایجاد گذرواژه‌هایی برای ایمن نگه داشتن اطلاعات شما می‌پردازیم.

گذرواژه‌های قوی:

این گذرواژه‌ها مبتنی بر یک عبارت یا جمله توصیفی بوده که به خاطر سپردن آن آسان و حدس زدن آن برای دیگران دشوار است و عباراتی مانند حروف اول کلمات آهنگ مورد علاقه شما، اولین حروف کلمات یک جمله خاص و یا ترکیبی از حروف، اعداد و نمادها را شامل می‌شود. به طور مثال، «went to Western Elementary School for grade 3» می‌تواند برای ایجاد رمز عبوری مانند lw2We\$t4g3 استفاده شود.

گذرواژه‌های متوسط: گذرواژه‌هایی هستند که قوی بوده و حدس زدن آن برای نرم‌افزارهای مخرب آسان نیست، اما ممکن است توسط شخصی که شما را می‌شناسد قابل حدس زدن باشند (به طور مثال lwenttoWester).

گذرواژه‌های ضعیف: این گذرواژه‌ها اغلب شامل اطلاعات شخصی مانند نام حیوان خانگی بوده و به راحتی می‌توان آن‌ها را هک کرد و یا توسط شخصی که شما را می‌شناسد به راحتی قابل حدس زدن هستند (به طور مثال «loveBuddy» و یا «likechocolate»).

بایدها

در ادامه ایده‌ای به منظور ایجاد یک گذرواژه بسیار امن ارائه شده است:

- برای هر یک از حساب‌های مهم خود از گذرواژه متفاوتی استفاده کنید.
- هر گذرواژه بایستی دست کم از هشت کاراکتر ساخته شده باشد. هر چه طولانی‌تر، بهتر! (تا حدی که بتوانید آن را به خاطر بسپارید!).
- از ترکیب حروف (بزرگ و کوچک)، اعداد و نمادها استفاده کنید.
- گذرواژه‌های خود را حفظ کنید تا نیازی به نوشتن آنها نداشته باشید زیرا کار خطرناکی است.
- اگرگمان کردید شخص دیگری از گذرواژه شما باخبر شده است (به جز والدین یا سرپرستان)، فوراً آن را تغییر دهید.
- گذرواژه‌های خود را هر از چند گاهی تغییر دهید.
- همیشه از قفل صفحه نمایش قوی برای دستگاه‌های خود استفاده کنید. دستگاه‌های خود را طوری تنظیم کنید که در صورت قرار گرفتن در دستان فردی ناشناس سریع قفل شوند.
- برای به خاطر سپردن گذرواژه‌های خود از مدیریت گذرواژه استفاده کنید. به این ترتیب می‌توانید برای هر یک از حساب‌های خود از یک گذرواژه منحصر به فرد استفاده کنید و مجبور نباشید همه آنها را به خاطر بسپارید.

نبایدها

- از اطلاعات شخصی (نام، آدرس، ایمیل، شماره تلفن، شماره بیمه، نام کوچک مادر، تاریخ تولد یا حتی نام حیوان خانگی و غیره) برای گذرواژه خود استفاده نکنید.
- از گذرواژه‌ای استفاده نکنید که حدس زدن آن ساده باشد، مانند نام مستعار، شکلات، نام مدرسه، تیم ورزشی مورد علاقه، یک رشته اعداد (مانند 123456)، و غیره و قطعا از کلمه «Password» نیز استفاده نکنید!
- گذرواژه خود را با کسی غیر از والدین یا سرپرست خود به اشتراک نگذارید.
- هرگز گذرواژه را جایی که کسی بتواند آنها را پیدا کند، یادداشت نکنید.

در حفظ اسرار خود کوشا باشید: درس 3

پیش خودت نگاهش دار.

معلم از رایانه مدرسه استفاده کرده تا نشان دهد برای سفارشی سازی تنظیمات حریم خصوصی خود باید چه کار کرد.

اهداف درس برای دانش آموزان

- ✓ سفارشی سازی تنظیمات حریم خصوصی سرویس های آنلاین خود
- ✓ تصمیم گیری در خصوص به اشتراک گذاری اطلاعات در سایت ها و سرویس های آنلاین خود
- ✓ آشنایی با مفهوم راستی آزمایی های دو مرحله ای و دو عاملی و زمان استفاده از آن.



بیا یاد حرف بزنیم



حریم خصوصی + امنیت

حریم خصوصی آنلاین و امنیت آنلاین دست به دست هم می دهند. اکثر برنامه ها و نرم افزارها راه هایی برای کنترل اطلاعاتی که به اشتراک می گذاریم و چگونگی آن را ارائه می دهند.

وقتی از یک برنامه یا وبسایت استفاده می کنید، به دنبال گزینه ای مانند «حساب من» یا «تنظیمات» باشید. در این قسمت ها است که می توانید حریم خصوصی و امنیتی را تنظیم کرده تا به شما امکان تصمیم گیری در موارد زیر بدهند:

- چه اطلاعاتی در صفحه یا نمایه شما قابل مشاهده باشد؟
- چه کسی می تواند پست ها، عکس ها، ویدیوها یا سایر محتوایی که به اشتراک می گذارید را مشاهده کند؟

یادگیری استفاده از این تنظیمات برای محافظت از حریم خصوصی خود و به روز نگه داشتن آنها به شما کمک خواهد کرد تا حریم خصوصی، امنیت و ایمنی خود را مدیریت کنید.

علاوه بر تنظیمات، آنچه اهمیت بسیار دارد این است که چه کسی می تواند جزو دوستان یا دنبال کنندگان شما باشد (که ممکن است در تنظیمات شما باشد یا نباشد). ایمن ترین راه این است که فقط خانواده و فهرست دوستانتان بتوانند شما را دنبال کنند. فراموش نکنید اگر به افراد دیگر اجازه دهید شما را دنبال کنند هر آنچه که به اشتراک می گذارید توسط افرادی که هرگز با آنها آشنایی نداشته اید قابل مشاهده است. این موضوع ممکن است کمی ترسناک باشد و گاهی والدین اصلاً اجازه چنین کاری را نمی دهند. با بزرگسالی که به وی اعتماد دارید صحبت کنید تا بفهمید چه چیز برای شما بهتر است و چه چیز امنیت شما را حفظ کرده و باعث آرامش شما می شود.

والدین یا سرپرست شما باید برای تصمیم گیری در چنین مواردی کنار شما باشند. همچنین انجام تنظیمات حریم خصوصی در کنار والدین یا سرپرست شما می تواند سرگرم کننده باشد (تا آنها بتوانند ببینند چقدر باهوش هستید!)

فعالیت



وسائل مورد نیاز:

• یک رایانه که به یک پروژکتور متصل است و می‌تواند حساب کاربری که برای نمایش در کلاس مناسب است را نمایش دهد (مثلاً ایمیل موقت یا حساب کلاس)

بررسی گزینه‌ها

من رایانهٔ مدرسه را به صفحه نمایش وصل کردم. بیایید به صفحه تنظیمات این برنامه بروید، جایی که می‌توانیم گزینه‌های خود را ببینیم. با من از طریق (دانش‌آموزان خود را تشویق کنید تا به شما کمک کنند) صحبت کنید.

• تغییر گذرواژه

• عمومی یا خصوصی کردن صفحه یا نمایه آنلاین خود، از جمله عکس‌ها و ویدیوهای شما (فقط برای خانواده و دوستانی که انتخاب می‌کنید قابل مشاهده باشد).

• بررسی موقعیت مکانی و سایر تنظیمات، کدام یک برای شما بهتر است؟

• دریافت هشدار در صورتی که فردی بخواهد از یک طریق یک دستگاه ناشناس وارد حساب کاربری شما شود.

• دریافت هشدار زمانی که شخصی شما را برچسب گذاری (تگ کردن) کند.

• فعال کردن تأیید دو مرحله‌ای یا دو عاملی

• تنظیم اطلاعات بازیابی در صورت قفل شدن دسترسی به حساب خود

گزارش مشکلات

این که کدام یک از تنظیمات حریم خصوصی و امنیتی برای شما مناسب‌تر است موضوعی است که بایستی با والدین یا سرپرست خود در میان بگذارید. اما همیشه به یاد داشته باشید که مهم‌ترین تنظیمات امنیتی در مغز شما است و هرچه بزرگ می‌شوید، بیشتر و بیشتر تصمیم می‌گیرید چه مقدار اطلاعات شخصی خود را، آن هم چه زمانی و با چه کسی به اشتراک بگذارید. بنابراین آنچه بیش از هر چیز اهمیت دارد این است که از همین الان به این نوع تصمیم‌گیری عادت کنید.

نکته:

انتخاب یک گذرواژه قوی و منحصر به فرد برای تمامی حساب‌های خود اولین گام مناسبی است که باید بردارید. حال باید گذرواژه‌های خود را به خاطر بسپارید و آنها را خصوصی نگه دارید.