

## شبکه های اجتماعی

چیزهایی که باید بدانم !



Co-funded by  
the European Union



**help**   
saferinternet **line**  
**210 6007686**

خط محتویات غیرقانونی

**safeline**   
[www.safeline.gr](http://www.safeline.gr)

خط درخواست کمک

# سایت های شبکه های اجتماعی

شبکه های اجتماعی تعامل بین افراد را امکان پذیر می کنند ، به کاربران امکان ایجاد پروفایل های شخصی ، برقراری ارتباط با سایر اعضای سرویس و همچنین به اشتراک گذاشتن انواع فایل های دیجیتال ( موسیقی ، عکس ، متن و غیره ) و همچنین افکار و احساسات شخصی را می دهند. بخاطر امکانات فراوانی که در اختیار کاربران خود قرار می دهند ، شبکه های اجتماعی مفهوم ارتباط را در عصر مدرن به شدت تغییر داده اند و بطور قابل توجهی بر روابط انسانی تاثیر گذاشته اند. یک مشخصه مهم دیگر این است که میزان انتشار و تثبیت آنها به ویژه در بین جوانان بسیار بالاست



## مراقب چه چیزی باید باشم ؟

### افشای داده های شخصی

بسیاری اوقات حتی اگر بسیار مراقب هم باشیم و از داده های شخصی خود محافظت کنیم ، نمی توانیم آنچه را که سایر کاربران از طریق پست های خود در مورد ما فاش می کنند کنترل کنیم . همچنین ، با به اشتراک گذاشتن یک عکس می توانیم بدون اینکه متوجه باشیم ، داده های خود را فاش کنیم

### ایجاد یک شهرت بد در اینترنت

هر چیزی که در اینترنت آپلود می کنیم ، حتی اگر بعداً آن را حذف کنیم دیگر خارج از کنترل ما است زیرا نمی دانیم چه کسی آن را ذخیره کرده است و چگونه از آن استفاده خواهد کرد. همچنین ، هر کسی می تواند از مطالب یا نظرات اشخاص ثالث که در اینترنت پست شده اند ، نظر منفی برای ما ایجاد کند. واقعیتی که می تواند برای ما در روابط و پیشرفت هزینه ایجاد کند

### زور گویی در اینترنت

مطالب و نظراتی که با دیگران به اشتراک می گذاریم می توانند توسط کاربران مخرب برای آزار و اذیت یا تهدید ما استفاده شوند.

## رد یابی موقعیت مکانی

با افشای موقعیت مکانی خود در برابر کاربران مخربی که ممکن است از این اطلاعات برای آسیب رساندن به ما استفاده می کنند ، آسیب پذیر می شویم

## اغواگری اینترنتی

در اینترنت بسیار آسان است که فردی در مورد اینکه واقعاً چه کسی هست دروغ بگوید و شروع به گفتگو از طریق اینترنت با هدف جلب اعتماد ما کند تا قبول کنیم که او را در دنیای واقعی ملاقات کنیم و در ادامه بتواند از ما سوء استفاده کند

## جعل هویت

هرکسی که به پروفایل ما دسترسی داشته باشد می تواند نام و نام خانوادگی ، عکس ، سایر اطلاعات ما را << سرقت کند >> و از آنها با اهداف مخرب استفاده کند. همچنین، اگر به رمزهای ورودی ما دسترسی داشته باشد می تواند خود را به جای ما معرفی کند و از این طریق برای سایر کاربران مشکل ایجاد کند

## ارائه مشخصات به برنامه ها / شرکت ها

بسیاری از پلتفرم های شبکه های اجتماعی دارای برنامه هایی هستند که همیشه امن نیستند و برای فعال شدن، آنها نیاز به داده های شخصی ما دارند که ما نمی دانیم توسط چه کسی و به چه روشی بعداً از آنها استفاده خواهد شد. اطلاعات شخصی ما را اکثراً در اختیار شرکت ها قرار می دهند و بدون درخواست ما از آنها برای تبلیغات هدفمند و سایر اهداف دیگر استفاده می شوند



## توصیه های اساسی ...

## قواعد استفاده

قبل از اقدام به ایجاد یک پروفایل در شبکه های اجتماعی توصیه می شود که قواعد استفاده و خط مشی امنیتی آن را به دقت مطالعه کنید. اگر با برخی از این قواعد موافق نیستیم ، ثبت نام خود را ادامه نمی دهیم . حتی اگر با این مقررات موافقت کرده و حساب کاربری خود را باز کنیم میبایستی هر از گاهی به قواعد و مقررات استفاده نگاهی بیندازیم زیرا سرویس دهندگان این حق را دارند که در هر زمان و بدون اطلاع قبلی آنها را تغییر دهند.

## حفاظت از داده های شخصی

تنظیمات امنیتی و حریم خصوصی خود در پروفایل مان را چک می کنیم . باید بگونه ای آنها را تنظیم کنیم که پروفایل و پست های ما فقط برای دوستانمان قابل مشاهده باشند. از دوستان خود می خواهیم که بدون رضایت مطالبی که مربوط به ما می شوند را منتشر نکنند. به برنامه ها هرگونه استفاده از مشخصات شخصی خود را نمی دهیم تا در پروفایل ما منتشر کنند.

قبل از پست گذاشتن فکر می کنیم

قبل از اقدام به گذاشتن پست در شبکه های اجتماعی خوب است که در نظر داشته باشیم که حتی اگر آن پست را حذف کنیم دیگر از کنترل ما خارج شده است و می تواند برای همیشه در فضای مجازی باقی بماند و ما را نمایندگی کند. همچنین به این فکر می کنیم که کسانی که آن را می خوانند چه احساسی خواهند داشت و چه تاثیری ممکن است بر زندگی دیگران یا در مسیر آینده خودمان بگذارد، چنانچه پست ما درباره شخص دیگری است یا اطلاعاتی درباره او فاش می کند، ابتدا رضایت او را جلب کرده و بعد آن را به اشتراک بگذاریم.



## به غریبه ها اعتماد نداریم

ما مراقب این هستیم که چه کسانی را به عنوان دوست در فضای مجازی خود می پذیریم و با چه کسانی صحبت می کنیم. هرگز نمی پذیریم که کسی را که در زندگی واقعی خود نمی شناسیم ملاقات کنیم و اطلاعات ، عکس ها یا ویدئو های تحریک آمیز در فضای مجازی تبادل نمی کنیم زیرا نمی دانیم ممکن است بکجا ختم شوند و چگونه ممکن است مورد استفاده قرار گیرند.

## از رمزهای عبور خود محافظت می کنیم

از رمزهای عبور قوی استفاده می کنیم و آنها را برای کسی فاش نمی کنیم . برای هر حساب کاربری یک رمز عبور متفاوت استفاده می کنیم و بیاد داشته باشیم که آن را به صورت دوره ای تغییر دهیم. اگر متوجه شدیم که حساب کاربری ما به خطر افتاده است آن را به مدیریت صفحه شبکه اجتماعی یا به سیف لاین گزارش می دهیم.

## مراکز اصلی گزارش شبکه های اجتماعی

<https://www.facebook.com/help/reportlinks> :FACEBOOK

<https://support.twitter.com/articles/2017463> :TWITTER

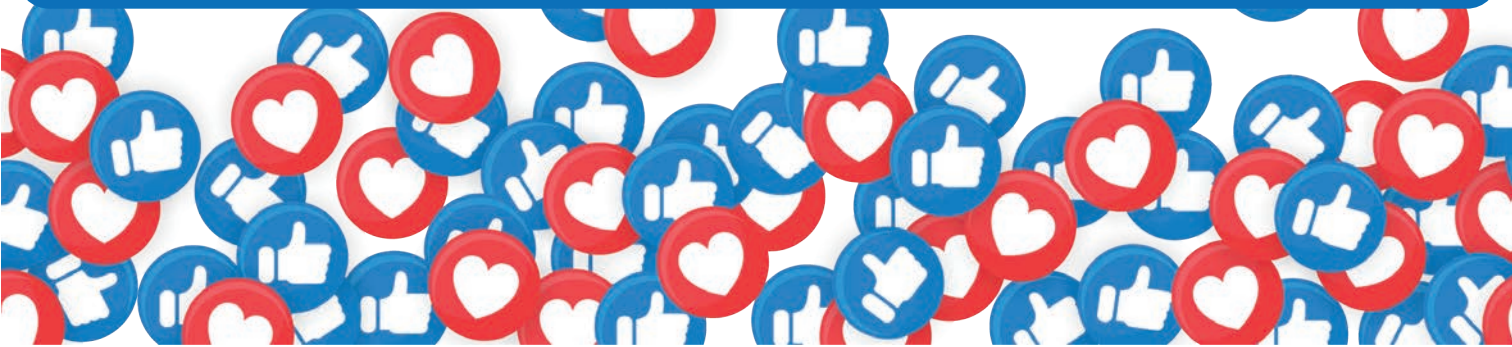
<https://www.youtube.com/yt/policyandsafety/el/reporting.html> :YOUTUBE

<https://www.facebook.com/help/instagram/454951664593304> :INSTAGRAM

<https://support.snapchat.com/en-US> :SNAPCHAT

<https://faq.whatsapp.com/en/android/21197244/?category=5245250> :WHATSAPP

<https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-default> :TIKTOK





از خطرات پنهان اینترنت مطلع  
شوید و یاد بگیرید که چگونه  
خود را در برابر آنها محافظت  
کنید



Co-funded by  
the European Union

مسؤولیت انحصاری این مقاله بر عهده نویسنده آن است. اتحادیه اروپا هیچگونه مسئولیتی در قبال هرگونه استفاده از محتویات این اطلاعات ندارد