Identity theft occurs when someone impersonates you using your personal information, such as your name, Social Security number, birthdate, etc., usually in order to commit a crime against you.

**Main types of identity theft that can impact you**

**Financial Identity Theft**
When someone utilizes the information of another person for financial benefit, this is known as financial identity theft. For example, someone might use your Social Security number to open a new credit card account or purchase something online.

**Social Security Identity Theft**
This type of theft occurs when your Social Security number is used to secure a job or obtain credit. Thieves may use it to pay back taxes, obtain assistance programs, or access government benefits. If you notice any unusual activity on your Social Security account, report it to the Social Security Administration immediately.

**Medical Identity Theft**
Thieves may use your personal information to obtain medical services, prescriptions, or bank account information. They might even pose as a representative from a health insurance company to get information such as Social Security numbers and dates of birth.

**Criminal Identity Theft**
This type of identity theft involves using someone else's personal identification in order to commit a crime against you. Some ways this can happen include using a stolen ID to purchase illegal drugs or using someone's information to claim unemployment benefits.

**Types of phishing attacks**

1. **Email/Website Phishing**
   - Thieves may send emails or create websites that appear to be legitimate but contain links to malicious websites.
   - They might try to trick you into giving out your personal information, such as usernames, passwords, or bank account numbers.

2. **Phishing via Social Media**
   - Phishers may create profiles on social media sites that mimic legitimate accounts.
   - They might post misleading links or requests for personal information.

3. **Phishing via Text Message (SMS)**
   - Thieves may send text messages that look like they come from a legitimate company or bank.
   - They might try to get you to click on a link or provide personal information in order to access your accounts.

**Ways to prevent identity theft**

1. **Use strong passwords**
   - A strong password is key to preventing identity theft.
   - Avoid using personal information such as your name, birthplace, or pet's name.

2. **Check your credit reports regularly**
   - You can check your credit report for free once a year by visiting AnnualCreditReport.com.
   - Look for any unfamiliar activity or accounts that might indicate identity theft.

3. **Use a Virtual Private Network (VPN)**
   - A VPN helps protect your online activity by encrypting your internet connection.
   - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

4. **Watch out for suspicious emails/websites**
   - Be cautious of emails or websites that seem suspicious or ask for personal information.
   - Check the URL of the site carefully to ensure it's legitimate.

5. **Protect your private documents**
   - Keep your personal documents secure and out of reach.
   - Shred important documents before discarding them to prevent identity theft.

6. **Use two-factor authentication**
   - Two-factor authentication adds an extra layer of security to your accounts.
   - This ensures that you are the only person who can access your accounts.

7. **Use a Virtual Private Network (VPN)**
   - A VPN helps protect your online activity by encrypting your internet connection.
   - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

8. **Use strong passwords**
   - A strong password is key to preventing identity theft.
   - Avoid using personal information such as your name, birthplace, or pet's name.

9. **Check your credit reports regularly**
   - You can check your credit report for free once a year by visiting AnnualCreditReport.com.
   - Look for any unfamiliar activity or accounts that might indicate identity theft.

10. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

11. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

12. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

13. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

14. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

15. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

16. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

17. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

18. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

19. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

20. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

21. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

22. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

23. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

24. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

25. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

26. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

27. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

28. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

29. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

30. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

31. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

32. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

33. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

34. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

35. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

36. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

37. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

38. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

39. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

40. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

41. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

42. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

43. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

44. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

45. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

46. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.

47. **Watch out for suspicious emails/websites**
    - Be cautious of emails or websites that seem suspicious or ask for personal information.
    - Check the URL of the site carefully to ensure it's legitimate.

48. **Protect your private documents**
    - Keep your personal documents secure and out of reach.
    - Shred important documents before discarding them to prevent identity theft.

49. **Use two-factor authentication**
    - Two-factor authentication adds an extra layer of security to your accounts.
    - This ensures that you are the only person who can access your accounts.

50. **Use a Virtual Private Network (VPN)**
    - A VPN helps protect your online activity by encrypting your internet connection.
    - Use a VPN when accessing public Wi-Fi networks to avoid identity theft.