



10 ways to protect yourself from online criminals

- Use Security Software**
Install and regularly update your anti-virus software and firewalls to prevent unauthorized access to your computer and protect your information such as account numbers and passwords.
- Be Wise About Wi-Fi**
Avoid accessing sensitive personal information on public networks/computers. Public Wi-Fi networks and computers at places such as restaurants or hotel business centers can be risky if they don't have up-to-date security software.
- Encrypt Your Data**
To guard your online transactions, look for a "lock" icon on the status bar of your internet browser the lock before you send personal or financial information online. It means your information will be safe when it's transmitted.
- Avoid Phishing Emails**
Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a virus or spyware that captures your passwords or other information you type.
- Be Alert to Impersonators**
Don't give out personal information unless you've initiated the contact. If you get an email asking for personal information, don't click on links in the email. Go to the company's site to contact them through their customer service.
- Be Discreet on Social Networking Sites**
Criminals comb those sites looking for information such as someone's place of birth, mother's maiden name or a pet's name, in case those details can help them guess or reset passwords for online accounts.
- Reduce Access to Devices**
Don't leave your computer or mobile device unattended and always lock your screen or log-off when finished. Use a device password or other method to control access to your device if it's stolen or lost.
- Keep Passwords Private**
Create "strong" passwords that are hard to guess, change them regularly, and try not to use the same passwords or PINs (personal identification numbers) for several accounts.
- Safely Dispose of Personal Information**
Before you dispose of a computer or mobile device, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.
- Include Children in Cybersecurity Planning**
Talk with your child about being safe online, including the risks of sharing personal information with people they don't know, and make sure the devices they use to connect to the Internet have up-to-date security.