Kids and Computer Security

The security of your computer can affect the safety of your online experience — and your kids'. Talk to your kids about what they can do to help protect your computer and your family's personal information.

Teaching Computer Security

Talk to your kids about:

- Protecting their personal information. Social Security numbers, account numbers, and passwords are examples of information to keep private.
- Watching out for "free" stuff. Free games, ring tones, or other downloads can hide malware. Tell your kids not to download anything unless they trust the source and they've scanned it with security software.
- Using strong email passwords and protecting them. The longer the password, the harder it is to crack. Personal information, your login name, common words, or adjacent keys on the keyboard are not safe passwords. Kids can protect their passwords by not sharing them with anyone, including their friends.

In addition, be sure your family computers are protected by reputable security software and use these basic computer security practices:

- **Update Your Software.** Keep your software – including your operating system, the web browsers you use to connect to the Internet, and your apps – up to date to protect against the latest threats. Most software can update automatically, so make sure to set yours to do so. Outdated software is easier for criminals to break into. If you think you have a virus or bad software on your computer, check out how to detect and get rid of malware.

- **Protect Your Personal Information.** Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about why someone needs it and whether you can really trust the request.

Kids and Computer Security

- In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

  Protect Your Passwords. Here are a few ideas for creating strong passwords and keeping them safe:

  - Use at least 10 characters; 12 is ideal for most home users.
  - Try to be unpredictable – don't use names, dates, or common words. Mix numbers, symbols, and capital letters into the middle of your password, not at the beginning or end.
  - Don't use the same password for many accounts. If it's stolen from you – or from one of the companies where you do business – thieves can use it to take over all your accounts.
  - Don't share passwords on the phone, in texts or by email. Legitimate companies will not ask you for your password.
  - If you write down a password, keep it locked up, out of plain sight.

  Consider Turning On Two-Factor Authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

  Give Personal Information Over Encrypted Websites Only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address. That means the site is secure.

  Back Up Your Files. No system is completely secure. Copy your files to an external hard drive or cloud storage. If your computer is attacked by malware, you'll still have access to your files.

Kids and Computer Security

P2P File Sharing

Some kids share music, games, or software online. Peer-to-peer (P2P) file-sharing allows people to share these kinds of files through an informal network of computers running the same software. P2P file-sharing has risks:

- You could accidentally provide many people with access to your private files.
- If your kids download copyrighted material, you could get mired in legal issues.
- A shared file could hide spyware, malware, or pornography.

Here are some tips to help your kids share files safely:

- Install file-sharing software properly. Activate the proper settings so that nothing private is shared.
- Before your kids open or play any file they've downloaded, advise them to use security software to scan it. Make sure the security software is up-to-date and running when the computer is connected to the internet.

Phishing

Phishing is when scam artists send fake text, email, or pop-up messages to get people to share their personal and financial information. Criminals use the information to commit identity theft.

Here are tips you can share with your kids to help them avoid a phishing scam:

- Don't reply to text, email, or pop-up messages that ask for personal or financial information, and don't follow any links in the message.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. Unexpected files may contain malware.

Get your kids involved, so they can develop their scam "antennas" and careful internet habits. Look for "teachable moments" — if you get a phishing message, show it to your kids. A demonstration can help them recognize a potential phishing scam and help them understand that messages on the internet aren't always what they seem.

Kids and Computer Security

Apps

Do you — or your kids — download "apps" to a phone or social networking page? Downloading may give the app's developers access to personal information that's not related to the purpose of the app. The developers may share the information they collect with marketers or other companies. Suggest that your kids check the privacy policy and their privacy settings to see what information the app can access. And consider this: Is finding out which cartoon character you are really worth sharing the details of your life — or your children's?