ConnectSafely

QUICK-GUIDE TO

Cybersecurity

Why should we care about security?

Insecure devices and accounts can jeopardize your privacy, financial well-being and even personal safety. And it can affect others because insecure devices can spread malicious software to other people's devices via the internet.

What are the most important steps to take?

Create (and don't share) strong passwords, be careful where you click, use security software, keep your operating systems and apps up-to-date, be careful what apps you install and don't fall for scams.

Are kids and teens at high risk?

Yes. Young people are very vulnerable to hacks and scams. Not only are they online a lot, but they tend to be curious and adventurous — good qualities that can lead them into problematic places. Youth are especially vulnerable to identity theft because they usually have a clean credit record, and a fake identity is harder to detect.

What is 2-Factor Authentication?

Like an ATM card, two-factor authentication, sometimes called “multi-factor authentication," requires that you know something and have something. What you "know" is your password and what you "have" is typically a cell phone. If you try to sign into a site or app from an unknown device, you'll get a code sent to your phone, which you have to type in to gain access. **We recommend using 2-factor authentication whenever possible, as it significantly reduces the chance of someone remotely accessing your accounts.**

How can I come up with an easy-to-remember password?
Come up with a unique phrase like "I met Susie Jones at Lincoln High School in 2012," and use the first letter of each word + numbers and a symbol. Your password could be ImSJaLHSi#12, but change it up for each site by adding a letter or two. Also, consider using a password manager that will remember your passwords for you. More at ConnectSafely.org/passwords.

What is “phishing?” Phishing is when you get a link in an email that appears to be from a legitimate site such as your bank or school. Perhaps it will say your security is at risk and you have to log in to change your password. But the link sends you to a rogue site whose purpose is to get your user credentials or trick you into providing a credit card or other personal information. It's a major way that hackers compromise accounts.

More Advice for Staying Safe

Be careful where you click. Fake or malicious websites (or legitimate ones that criminals have hacked) can jeopardize your device and the data on it. Sometimes called "drive-by downloads," these sites can install malicious software onto your device if you visit them or perhaps click on the sites' links. Often they look legitimate, offer something too good to be true or contain some type of "forbidden" content such as sexually explicit material, gambling or free movies or music. Then there's "clickjacking" — bogus links on social media pages that have been hacked. They appear to link to something tantalizing but instead redirect you to a site that contains spam advertising, plants malware on your device or posts bad links on your profile.

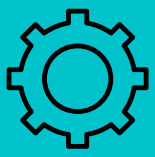
Keep software and apps up-to-date. Regardless of whether you're using a computer or a mobile device, it's vital to keep your operating system and software (or apps) current because developers fix security flaws and vulnerabilities with updates. Turn on automatic updates for your operating system and browsers if you haven't already. And if you update an app or program, recheck your privacy settings to ensure they haven't gone back to the default settings.

Watch out for scams. There are many types of online scams including fake charities, posts appearing to be from "friends" or "family" asking for money and appeals for help after a disaster. If you get a charity appeal, find out the organization's actual web address and go there directly.

Use caution before downloading. A common way criminals plant malware on devices is to get you to download an app, piece of software, or a document (such as a PDF) that may contain malicious computer code. Only download apps from legitimate app stores such as the Apple App Store or Google Play Store. Read reviews or at least user ratings. The same goes for software. Avoid random software download sites and instead use legitimate ones like Download.com or the sites associated with known computer or software companies.

Use an anti-malware program or app. There are excellent anti-malware apps for personal computers and mobile devices. You'll find a list of reputable vendors at ConnectSafely.org/security.

For more info on passwords, visit ConnectSafely.org/passwords



Fake or malicious websites (or legitimate ones that criminals have hacked) can jeopardize your device.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

Revised 7/7/21