Cyber Challenge Checklist

Keep your accounts and your devices safe!

- [ ] Change your passwords/passphrases
- [ ] Enable two-factor or multifactor authentication
- [ ] Lock your device
- [ ] Don't overshare on social media
- [ ] Back up your files
- [ ] Use a security-conscious email provider
- [ ] Install security updates
- [ ] Delete unused apps
- [ ] Watch where you click
- [ ] Use a password/passphrase manager

Cyber Challenge Checklist

Whether it's Windows or Mac, Android or iPhone, ALL internet-connected technology is prone to vulnerabilities. Malicious cyber actors are constantly seeking ways to exploit any opportunity to get in your systems, such as through out-of-date software, unsecure apps that leave your data exposed, or easy-to-guess passwords.

However, you do not need to be a cybersecurity expert to help yourself and members of your community protect themselves.

Here are four simple steps everyone should take to enhance cybersecurity at home and in the workplace:

- **Think Before You Click**: Recognize and Report Phishing: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software**: Don't delay -- If you see a software update notification, act promptly. Better yet, turn on automatic updates.
- **Use Strong Passwords/Passphrases**: Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, strong passwords for each of your accounts. A password manager will generate, securely store, and enter passwords for you!
- **Enable Multi-Factor Authentication**: You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.

Want to learn more? Keep reading!

Improve your passwords/passphrases

Nothing you do online is safe unless you use strong passwords that actually protect your information.

Most people use the same password everywhere, and their password is easy to guess. You'd be amazed how many people use the password "ABC123" or "12345". Using a password like this is basically asking to be hacked.

Passwords like "Rover2015" and "R0v3r2015" are actually the same strength. This is because their length is the same. For real protection, use LONGER passphrases. Each additional character increases the amount of time for a hacker with a supercomputer to guess your passphrase. A 16-character alphabetic passphrase is much stronger than an 8-character password with special characters. Of course, even with a long passphrase, you can always add in special characters to make it harder to guess.

In addition to creating strong passwords, you unfortunately must use a different password for each web site you use. If a hacker does get access to one of your passwords, you don't want them to get into ALL your accounts.

A few years back, hackers got access to EVERY password at a popular social networking site and they published all these logins online for anybody to see. If your login was published, anybody in the world can now access your account on any website where you use that same password.

If it seems like a huge burden to remember all your new, longer passwords, that's because it is. But there are tools you can add to your browser that can make this easier. Whether you use a browser add-on or not, it's absolutely critical to use longer passwords, and a different password on every web site.

Enable two-factor or multifactor authentication

This next one makes a big difference! Enable multifactor authentication wherever possible, especially for your most sensitive data -- like email, social media, or cloud storage accounts.

Two-factor authentication, or higher security options like multifactor authentication, adds extra security to your passphrase. So even if somebody knows your passphrase, they need something else to log in as you. Often this is a security code that's sent to your phone, which means somebody needs your passphrase AND your phone to login. All major email or social networking sites offer this security feature. When they do, you should use it.

Lock your device

If you lose your device, you don't want to add insult to injury by leaving yourself vulnerable to someone stealing your information. Provide an initial layer of security by locking your phone with a password or a PIN number — preferably one that's longer than four numbers.

Don’t overshare on social media

No, we’re not talking about pictures of what you ate for lunch. Don’t post confidential information like your home address, phone number, and credit card number. Collecting even a few tidbits of your personal information makes it easier for someone to pretend to be you and use your accounts without your permission and steal your data.

Back up your files

In the event you do encounter malware or a virus, make sure you don’t lose access to documents you need. Back up your important files, using a cloud service or a physical hard drive.

Use a security-conscious email provider

Make sure your email provider has strong spam blocking and features like multi-factor authentication.

Install security updates

Every computer that's connected to the internet is frequently being attacked by hackers who test to see if the computer is prone to any known vulnerabilities. The only way to be safe is to always have the latest security updates installed. If you see a software update notification, act promptly. Better yet, learn how to turn on automatic updates.

Delete unused apps

Not only will deleting unused apps free up more space on your device, but it can also protect your information. Apps on your phone or computer that are no longer supported by the developer open you up to security risks. Plus, most apps collect data about you — why give your data to an app you're not using?

Watch where you click

Don’t click on ads that offer prizes, money, or something for free. Similarly, don’t click on suspicious links — use your mouse to hover over a link to see where it’s about to take you.

In your inbox, don’t open email from people you don’t know or download attachments from an email you didn’t expect to get. Be suspicious of emails asking you to login somewhere — check for grammatical errors, a low-quality logo or a lack of a logo, a strange URL, or other indicators of a phishing attempt.

Use a password/passphrase manager

Let's review. For real protection, it’s much more valuable to use LONGER passwords than short but complex passwords. In addition to creating strong passwords, you unfortunately must use a different password for each web site you use. That covers the rule that they have to be long, and unique. The third rule is that to be strong, they should be randomly generated, like by rolling dice or on a computer.

If it seems like a huge burden to remember all your long, unique, and random passwords or passphrases, that’s because it is. But, there are tools called password managers that can generate these strong password and securely store them. But what’s especially great is that they can also enter them into login pages.

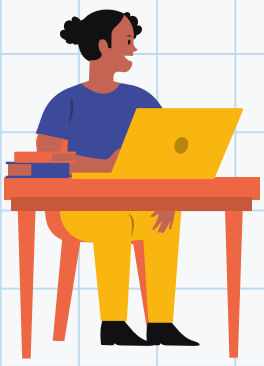
Tips for Students

Only download apps with an adult's permission

Check with your parent, guardian, or teacher before downloading an app to your device.

Don't give out personal information

Ask your parent, guardian, or teacher for help if an email or someone online asks you for your full name, address, birthday, or phone number.

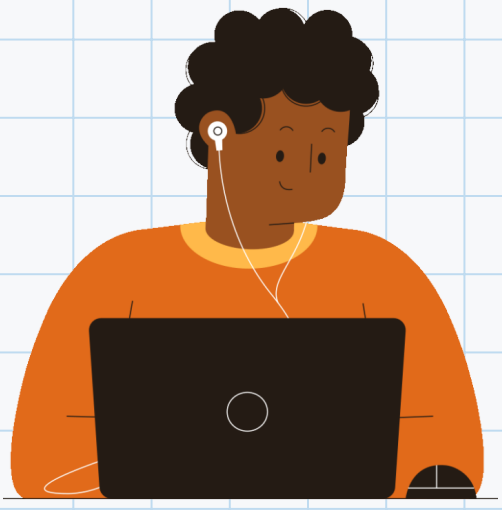


Use strong passwords

Don’t include your name, birthday, or other information that can be guessed in your password. Instead, make long passwords — they can include numbers, special characters, or even be phrases you’ll remember. Use different passwords on all of your accounts — a parent, guardian, or teacher can help you set up a password manager to remember them all!

Watch where you click

Don’t open emails from people you don’t know. Don’t click on ads that offer prizes, money, or something for free.



Check your settings

Have a parent, guardian, or teacher help you make sure the privacy settings on an apps or social media platforms you use are set and appropriate for your age group.

Take care of your tech

Don’t open emails from people you don’t know. Don’t click on ads that offer prizes, money, or something for free.