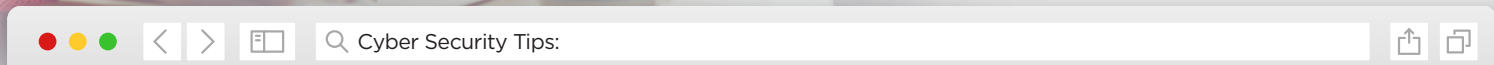




# CYBER SECURITY

## WHEN WORKING FROM HOME

When working remotely, it's important to stick to the same cyber safety guidelines as though you were in the office. With the FBI reporting an uptick in cyber crime related to coronavirus,<sup>1</sup> it's important to stay vigilant while connected at home.



### Use Strong Passwords

Passwords for WiFi and work accounts should be unique and tough to crack. Start with a special phrase that is at least 12 characters. Incorporate uppercase and lowercase letters, numbers and special characters. Avoid including personal information, and don't use the same password for everything.



### Double Up on Security



Multi-factor authentication gives your work accounts an extra layer of security. This feature requires you to confirm your identity by way of another device when logging in somewhere new. Also consider requiring a password for online video conference calls.



### Updates Matter

Install the latest updates for all devices, programs and apps, which typically include improved security measures. Where possible, opt for automatic updates.



### Consider a VPN

If your company does not use a Virtual Private Network (VPN), consider investing in your own. This software secures your network to reduce your risk of a hack. Popular services include NordVPN and ExpressVPN.

New message



## Watch Out for Fake Emails!!!

Cc Bcc

Hackers often target individuals first with personalized fake emails, or phishing emails. Before you act:

#### Review the Sender's Email Address:

It may look like a message from your bank or a colleague, but a misspelled or incorrect email address indicates it's fake.

#### Hover, Not Click:

Place your cursor over the link to read the URL. An unrecognizable site is a big red flag, so don't click it.

#### Check the Tone:

Urgent, fearful messages requiring immediate action and a deadline are typically fake — even if they look like they're from a co-worker.

#### Report It:


Notify your IT department immediately of the message following company protocol.

# KEEPING YOUR KIDS SAFE ONLINE

With schools moving to virtual learning and limits on outdoor activities, kids are spending a lot more time online. Here are some tips to help make sure they use their devices safely.




Tips to keep kids safe online



## Know What Your Kids Are Up To


Understand your kids' Internet habits. Know what sites they visit for school and for fun, and talk to them if you see something unusual.

https://youtube.com/kids




### PRO-TIP:

For the little ones, try installing YouTube Kids instead of normal YouTube on their device.



## Block Dangerous Websites

Talk to your Internet provider if you want to block certain websites from your network.



## Set the Ground Rules

Consider asking your kids to stay nearby when they're using their devices and setting rules for what sites they can visit and when — i.e. YouTube allowed after school hours only.

Welcome to Live Chat!

## Have a Conversation

- Outline the rules and set expectations for responsible online behavior.
- Educate kids on cybersafety so they understand for themselves the risks of unfamiliar websites, mysterious downloads and conversations with strangers on the web.
- Share tips on creating strong passwords, protecting personal information and using social media safely — especially relevant for teens and tweens.

Please write your message and press the Send button...