

Take a well-being break

Spot and avoid cyber scams

You're probably catching up with all your emails and using social media to stay in touch, while staying safe at home. It's important to have that connection. We understand and want to help you avoid cyber scammers looking to take advantage of concerns over COVID-19.

These tips can help you protect your personal data and avoid becoming a victim of online crime:



Watch for unsafe emails. Avoid clicking on links in emails asking you to update your personal information. Be careful about opening email attachments. And be suspicious of promises of free gifts or prizes.



Use trusted sources for information about COVID-19. Look for sites ending in .edu (for education) or .gov (for government), including [CDC.gov](https://www.cdc.gov) and [coronavirus.gov](https://www.coronavirus.gov).



Don't share personal or financial information. Never give your bank account number, Social Security number or date of birth to an unknown source.



Shop online safely. Make sure the website starts with "https." The "s" stands for secure. Look for the padlock icon next to the web address (URL), which lets you know the site uses encryption. Type new website URLs directly into the address bar instead of clicking on links or cutting and pasting from an email.



Make sure charities are legal. Before you reach for your wallet, go to [Federal Trade Commission Consumer Information](https://www.ftc.gov/consumer) and check the charity.



For extra support

Here are some resources to check out:

- Your company's Employee Assistance Program (EAP) for identity theft
- [The U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency \(CISA\)](https://www.dhs.gov/cybersecurity)
- [The Federal Bureau of Investigation Scams and Safety on the Internet](https://www.fbi.gov/scams-safety)
- [The Federal Trade Commission OnGuard Online.](https://www.ftc.gov/online)

