EMAIL SAFETY

WHAT IF YOU ARE HACKED?

You might have been hacked if:

- Friends and family are getting emails or messages you didn't send.
- Your 'Sent' messages folder has messages you didn't send, or it has been emptied.
- Your social media accounts have posts you didn't make.
- You can't log into your email or social media account.

1 UPDATE YOUR SYSTEM AND DELETE ANY MALWARE.

The first thing you should do if your account gets hacked is to run an end-to-end antivirus scan. Also, set your security software, internet browser, and operating system to update automatically.

2 REVIEW SOCIAL MEDIA ACCOUNTS.

Look for changes on your social networking sites, look for changes to the account since you last logged in. Look at your personal details and review any third-party apps connected to your account.

3 CHANGE YOUR PASSWORDS.

Choose a new password that is very different from your old one and make sure it doesn't contain strings of repeated characters or numbers. Your password should be unique for each account.

4 CHANGE YOUR SECURITY QUESTIONS.

While your password was the most likely attack route, it's also possible that hackers broke into your account after answering your security questions. In order to further protect your email, be sure to employ the multi-factor authentication.

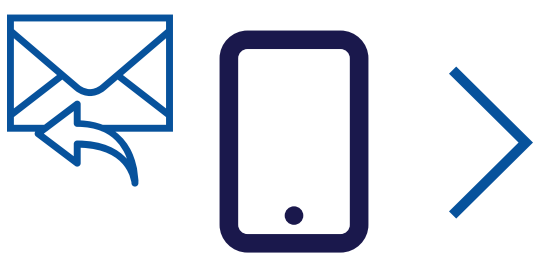
5 REPORT THE HACK.

If you haven't already, contact your email provider and report the hack. This is important even if your hacked email didn't cause you to lose access since it helps providers track scam-based behavior.

6 MANAGE YOUR EMAIL ACCOUNTS.

When you are checking your email at a public computer, you need to log out of your email and close the browser window completely.

7 EMAIL THE RIGHT PEOPLE.



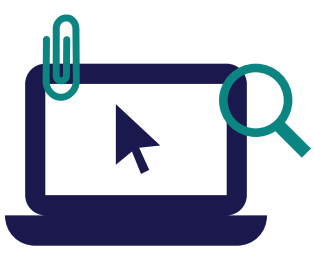
Be careful forwarding emails or replying to "all". Forwarding emails can create a significant security threat for yourself and the earlier recipients of the email.

8 AVOID BEING PHISHED.

Phishing is a type of online fraud wherein the sender of the email tries to trick you into giving out personal information or clicking on a link as a method to try to steal your identity or your money.

9 AVOID EMAIL MALWARE.

Don't always trust an email from someone you know. Scan all email attachments. Don't disable the email spam filter.



10 KEEP HACKERS AT BAY.

Don't share your account access information with others.
Don't use simple and easy-to-guess passwords.
Encrypt your important emails.

Contact your credit reporting agencies TransUnion and Equifax to monitor your accounts in the months after you've been hacked.