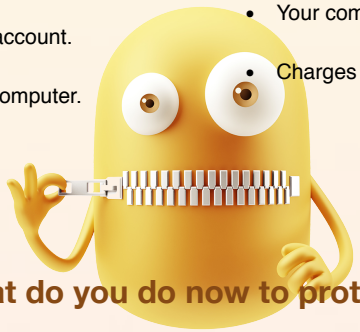
I've been HACKED ...now what?

How did you get hacked?

- You downloaded an email attachment that infected your computer or smartphone.
- You download "free" software that looks useful but is actually dangerous.
- You used a public Wi-Fi network to check your email or surf the web.
- Your password was stolen when you "logged in" to a fake webpage that appeared real.
- You use the same password on more than one account.
- You're not using an anti-virus program on your computer.

What are signs you've been hacked?

- Your computer behaves oddly even after restarting.
- The navigation bar on your web browser suddenly has an extra row.
- Ads begin to appear in the middle of the screen on every webpage you visit.
- Your computer mouse moves when you're not using it.
- Your computer slows to a crawl (even slower than usual!).
- Charges you didn't make appear on credit or debit card statements.



What do you do now to protect yourself?

- Act fast. If it's a work computer, notify IT immediately. If it's a personal computer, follow these steps.
- Using a computer, tablet or smartphone that has not been infected, log into your online accounts — particularly email, banking and social media — as well as your home's Wi-Fi network and change the passwords. Make the new passwords are at least 12 characters long.
- Consider purchasing a password manager (such as 1Password, Dashlane, Keeper or OneLogin) to ensure your passwords are varied and safe.
- Do a Google search for free anti-virus software (such as McAfee, Avast, Bitdefender, Norton or Trend Micro). Download and use the software to scan and repair your personal computer.
- Using social media and email, alert your friends and colleagues not to accept invitations or open email attachments from you.
- Check your email — including the spam folder — to ensure new retail, email, social media and other accounts have not been set up in your name. You will need to keep checking on this regularly for months.
- Make sure your personal computer makes safety backups of the hard drive automatically, either using an external hard drive attached to your computer or backed up online using a cloud-based service (such as Carbonite, OpenDrive, Backblaze or Acronis).
- If a new account has been set up, visit the account, click "forgot password", and if you are able to change the password and get in, delete the account.
- In your web browser's settings, clear "cookies", "browsing data" and "browsing history."
- Do you own a smart electronic device that's connected to an app (such as a baby monitor, video doorbell, smart lock, home security camera and thermostat)? Just because it's new doesn't mean it's safe. Look up instructions online about how to change the device's default password.
- Visit the Federal Trade Commission's website to learn about preventing ID theft following a hack.
- Consider freezing or locking your credit at the three major credit reporting bureaus. Do a Google search to understand the pros and cons of those two choices.
- If you don't yet have a web account with the Social Security Administration or the IRS, set yours up so no one else can claim it.

AwareForce™