What to do if you have been hacked

- Scan your system and delete any malware. Make sure all software is up-to-date and set to update automatically. Keeping your security software, your internet browser, and your operating system up-to-date helps your computer keep pace with the latest threats.
- Immediately change all your passwords, if you can log into your accounts.
- Check the advice your email provider or social networking site has about restoring your account if you cannot log in. If your account has been taken over, you might need to fill out forms to prove your identity.
- Check your account settings to make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address.
- Tell your friends they might have gotten a malicious email from your account with a link or attachment that could install malware on their computers.
- More information: www.consumer.ftc.gov

cybersecurity.wa.gov

Office of CyberSecurity

The Washington State Legislature created the Office of CyberSecurity (OCS) in 2015 to provide strategic direction for cybersecurity and protect state networks from growing cyber threats.

The office and its team of cybersecurity experts work 24 hours a day to detect, block and respond to cyberattacks on state networks. The office helps prevent and mitigate threats before they can cause significant damage.

In addition, the office works with state, local government and military agencies to build more secure networks and has teams that can respond on a moment's notice to help agencies deal with cyber threats.

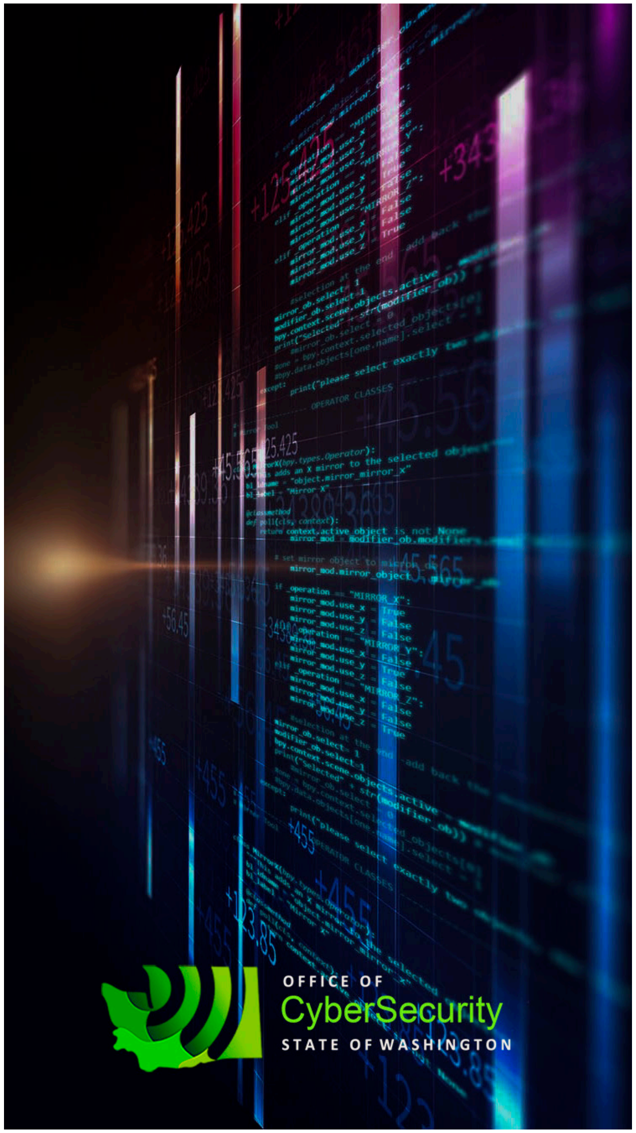
Our office also is working to make everyone more aware of cyber threats through educational outreach, holding public forums and providing tips and advice about how to stay safe online.

Contact information

Visit us:
1500 Jefferson St.
PO Box 41501
Olympia WA 98504
Email us:
cybersecurity@ocs.wa.gov
Call us:
360–407–8700
1–888–241–7597

Online: cybersecurity.wa.gov

Tips for keeping hackers out of your home, and your life



Staying safe while traveling

- Turn off auto-connect features on your devices that could connect you to an unencrypted network. Hackers set up such networks to prey on unsuspecting travelers.
- Make sure that any network you do connect to is encrypted and from a known source. For example, if you are at a hotel, check the name of its Wi-Fi network to ensure you connect to the correct one.
- Also make sure your phone's Bluetooth is turned off while traveling. Hackers can use it to connect to your phone and potentially hack it.
- Consider turning on your phone's GPS only when you need it to navigate to avoid alerting criminals to your whereabouts.

Securing your home network

- Change the SSID, or name of the network. Leaving the default name lets hackers know what kind of system you're using, and likely tells them the default login and password as well because that information is widely available.
- Given that, you should also change the default login and use a phrase several words long for the password.
- Turn on the highest level of encryption for your router, currently WPA2.
- Create a guest network for visitors that uses a separate password.
- Make sure to update the router firmware regularly. The updates will fix known security vulnerabilities that could allow hackers to access your network.

Protect yourself online

- Use one credit card for all online purchases to limit the potential for financial fraud. The Fair Credit Billing Act protects credit card use.
- In addition to using a login and password, add a layer of security by using "two-step" authentication that involves sending a code to your phone by text in order to login.
- Don't click on email links. That's how most hacks start. Go to company web pages directly, not from emails. If you recieve an unexpected attachement, call the sender to make sure they sent it.
- When making online purchases, look for "https" in the internet address (URL) . That shows the communication with the webpage is encrypted.