WHAT TO DO IF YOUR ONLINE ACCOUNTS KEEP GETTING HACKED

It's an all-too-common scenario. You've just changed your FaceBook, Twitter, or Email password. Just a few hours later, you start noticing signs that suggest that your account has been compromised again. How can you tell if your account has been accessed without your authorization? How can you prevent it from happening again, or stop the hacker from reading messages and sending replies on your behalf?

How can I tell if my account's been accessed?

Knowing what to look for can help you determine if any action is necessary. If you see any of the following, investigate further:

- Alerts that the password's been changed without your knowledge (note: if you get an email saying that your password's been changed, don't follow any links in the message itself. It might be phishing. Go to the site directly to view any alerts)
- Changed information in your profile or account settings
- Emails or messages that you didn't send
- New sign-in alerts
- The service shows multiple logged in instances. For example, gmail shows this on the bottom of your page under the "Last Account Activity" screen. Many other services have something similar. This may also allow you to log out of other locations.

Potential Causes and Solutions

Reusing passwords

Don't use the same password for multiple sites. Change your passwords and make sure they're unique.

Consider using a trusted password manager like Password Safe

Virus or malware

Use an online virus scanner like eset. You can also take your devices to trusted IT support.

Keylogger

A keylogger can come in two different forms. It may be a physical device plugged into your computer, often where the keyboard plugs in. It may also be an installed program. Look for any physical devices, then look at your installed apps or programs for anything you don't recognize. If you see anything out of the ordinary, seek trusted IT support.

Stored passwords in browsers, apps, or devices

Don't use password storage options. Remove browser extensions that store your passwords, and remove unused apps from your phone and browser plugins or extensions.

Easily answered password recovery questions

Don't use password recovery answers that anyone might be able to guess. Use alternate answers that you would remember. For example, an abusive partner would probably know the mother middle name or dog's name answers. Lie.

Unauthorized user has remote access to computer or device

Uninstall unknown or untrusted programs or apps, especially ones designed to enable remote access. Disable untrusted Facebook apps or other social media apps.

Remediation steps

These are the recommended fixes in order. If problem persists, move onto the next level

- Level 1
  - End other active sessions / logins
  - Change all of your passwords; use strong, unique passwords
  - Scan for malware
  - Look for keyloggers
  - Change your wifi password to kick off any unauthorized devices
  - Enable 2FA
  - Change security questions
  - Check password recovery settings to make sure that the recovery email / phone number actually belongs to you
  - Review security settings for impacted account(s). Many, like

facebook and gmail, have a security checkup option that will automatically review and recommend specific security settings
    - Consider contacting local law enforcement and the FBI (https://www.ic3.gov) as a crime has occurred (however, this may end up revealing your location if not already known)
    - If applicable, contact your victim advocate
- Level 2
    - Have your device(s) evaluated by a trusted IT professional
    - If anything is found. Consider contacting law enforcement right away. Of you choose to do that, do not make any changes to potentially preserve evidence.
    - change your passwords and security questions and look for keyloggers, enable 2FA
    - Uninstall your web browser if possible and reinstall a clean copy
- Level 3
    - Have any devices you use regularly reimaged (phone through factory reset; computers, reinstall operating system)
    - change your passwords and security questions, enable 2FA
    - Seek the services of an IT professional to look for other options

Prevention

- Use a password manager. We recommend https://pwsafe.org/
- Enable 2FA
- Use untrue security questions that you'll remember but your abuser won't guess
- Use strong passwords
- Don't fall for phishing scams
- Use different passwords for each site to prevent compromise of other accounts

- When signing up for accounts that you don't want to hear from, use a temporary email from a service like https://10minutemail.com
- Understand and use account security settings for each service
- Don't give out your password over the phone, email, or instant messaging
- Don't use computers you don't control to log into impacted accounts, until you're certain they're not infected or monitored