OnGuardOnline.gov

Hacked Email

You get a flood of messages from friends and family. They're getting emails from you with seemingly random links, or messages with urgent pleas to wire you money. It looks like your email or social media account might have been taken over. What do you do? For starters, make sure your security protections are up-to-date, reset your password, and warn your friends.

How You Know You've Been 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

In the case of emails with random links, it's possible your email address was "spoofed," or faked, and hackers don't actually have access to your account. But you'll want to take action, just in case.

What To Do When You've Been Hacked

1. Update your system and delete any malware

Make sure your security software is up-to-date

If you don't have security software, get it. But install security software only from **reputable, well-known companies**. Then, run it to scan your computer for viruses and spyware (aka **malware**). Delete any suspicious software and restart your computer.

Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically

Software developers often release updates to patch security vulnerabilities. Keep your security software, your internet browser, and your operating system up-to-date to help your computer keep pace with the latest hack attacks.

2. Change your passwords

That's IF you're able to log into your email or social networking account. Someone may have gotten your old password and changed it. If you use similar passwords for other accounts, change them, too. Make sure you **create strong passwords** that will be hard to guess.

3. Check the advice your email provider or social networking site has about restoring your account

You can find helpful advice **specific to the service**. If your account has been taken over, you might need to fill out forms to prove it's really you trying to get back into your account.

4. Check your account settings

Once you're back in your account, make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service, look for changes to the account since you last logged in — say, a new "friend."

5. Tell your friends

A quick email letting your friends know they might have gotten a malicious link or a fake plea for help can keep them from sending money they won't get back or installing malware on their computers. Put your friends' email addresses in the Bcc line to keep them confidential. You could copy and send this article, too.

What to Do Before You're Hacked

Use unique passwords for important sites, like your bank and email

That way, someone who knows one of your passwords won't suddenly have access to all your important accounts. Choose **strong passwords** that are harder to crack. Some people find password managers — software that stores and remembers your passwords for you — a helpful way to keep things straight. If you use a password manager, make sure to select a unique, strong password for it, too. Many password managers will let you know whether the master password you've created is strong enough.

Safeguard your usernames and passwords

Think twice when you're asked to enter credentials like usernames and passwords. Never provide them in response to an email. If the email or text seems to be from your bank, for example, visit the bank website directly rather than clicking on any links or calling any numbers in the message. Scammers impersonate well-known businesses **to trick people into giving out personal information**.

Turn on two-factor authentication if your service provider offers it

A number of online services offer "two-factor authentication," where getting into your account requires a password plus something else — say, a code sent to your smartphone — to prove it's really you.

Don't click on links or open attachments in emails unless you know who sent them and what they are

That link or attachment could install **malware** on your computer. Also do your part: don't forward random links.

Download free software only from sites you know and trust

If you're not sure who to trust, do some research before you download any software. Free games, file-sharing programs, and customized toolbars also could contain **malware**.

Don't treat public computers like your personal computer

If it's not your computer, don't let a web browser remember your passwords, and make sure to log out of any accounts when you're done. In fact, if you can help it, don't access personal accounts — like email, or especially bank accounts — on public computers at all. (Also be careful any time you use **public Wi-Fi**.)

July 2013