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
- What To Do When You've Been Hacked
- What To Do Before You're Hacked

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.)

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day—and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself.

How to Recognize Phishing

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

Here's a real world example of a phishing email.

Imagine you saw this in your inbox. **Do you see any signs that it's a scam?** Let's take a look.

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.
- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

While, at a glance, this email might look real, it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they're spoofing.

How to Protect Yourself From Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

Four Steps to Protect Yourself From Phishing

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.
2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.
3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you have—like a passcode you get via text message or an authentication app.
- Something you are—like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What to Do If You Suspect a Phishing Attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**
If the answer is "No," it could be a phishing scam. Go back and review the tips in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message and then delete it.
If the answer is "Yes," contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

What to Do If You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.
If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

How to Report Phishing

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing email, forward it to the FTC at spam@uce.gov and to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726).
Step 2. Report the phishing attack to the FTC at ftc.gov/complaint.
Tagged with: cyber security, phishing, scam

How to Spot, Avoid and Report Tech Support Scams

Share this page

- Facebook
- Twitter
- Linked-In

Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need, to fix a problem that doesn't exist. They often ask you to pay by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app because they know those types of payments can be hard to reverse.

- Spotting and Avoiding Tech Support Scams

Spotting and Avoiding Tech Support Scams

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

Phone Calls

Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist. Listen to an FTC undercover call with a tech support scammer.

If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.

Pop-up Warnings

Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.

Online Ads and Listings in Search Results Pages

Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help.

If you're looking for tech support, go to a company you know and trust.

2 Things to Know to Avoid a Tech Support Scam

1. Legitimate tech companies won't contact you by phone, email or text message to tell you there's a problem with your computer.

2. Security pop-up warnings from real tech companies will never ask you to call a phone number.

What to Do If You Think There’s a Problem With Your Computer

If you think there may be a problem with your computer, update your computer’s security software and run a scan.
If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

What to Do If You Were Scammed

If you paid a tech support scammer with a credit or debit card, you may be able to stop the transaction. Contact your credit card company or bank right away. Tell them what happened and ask if they can reverse the charges.

If you paid a tech support scammer with a gift card, contact the company that issued the card right away. Tell them you paid a scammer with the gift card and ask if they can refund your money.
If you gave a scammer remote access to your computer, update your computer’s security software. Then run a scan and delete anything it identifies as a problem.
If you gave your user name and password to a tech support scammer, change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

Avoid Tech Support Refund Scams
If someone calls to offer you a refund for tech support services you paid for, it’s likely a fake refund scam. How does the scam work? The caller will ask if you were happy with the services you got. If you say, “No,” they’ll offer you a refund. In another variation, the caller says the company is giving out refunds because it’s going out of business. No matter their story, they’re not giving refunds. They’re trying to steal more of your money. Don’t give them your bank account, credit card or other payment information.

Reporting Tech Support Scams

If a tech support scammer contacts you, report it to the Federal Trade Commission. When you report a scam, the FTC can use the information to build cases against scammers. Are you skeptical that reporting scams will make a difference? Watch this video to learn how your story could help the FTC stop scammers.

Tech support scams are common. In 2017, the FTC received more than 150,000 reports about these scamsfrom people like you. Add your voice. Report tech support scams to the FTC.

Now that you know how to recognize a tech support scam, share what you learned with someone you know. You might help them avoid a tech support scam.

Tagged with: computer security, cyber security, online security, scam