Hacked Accounts: What to Do Right Now

If you think your social media or email account has been hacked, wrestle it away from the bad guys by acting fast.

Hackers use a bunch of different tactics to try to compromise people's email, banking, social media, device, and other online accounts. Sometimes they do this to spam your friends with coupons, but other times they want to steal your money or identity. By alerting authorities and following a few steps, you can often retake control of your hacked account.

However, fast action is crucial. If you suspect that your digital account has been hacked, do something about it as soon as you can. Here's what you need to know right now!

How does an account get hacked?

Security breaches happen in many ways – sometimes you might click on a bad link, or the company in charge of the account could be attacked. This is why cybersecurity is so important to us all, and why we at the National Cybersecurity Alliance are so hyped up about it!

Commonly, an account is hacked through phishing. This is when cybercriminals use misleading emails, social media posts, phone calls, texts, or DMs that lure you to click on a bad link or download a malicious attachment. If you take the bait, the hackers can get access to your device or account.

Another common way your account could be hacked is if there is a data breach that reveals your username and password. The company controlling the account in question could be hacked, for example. If you reuse passwords, if any platform you use is compromised then cybercriminals might know your password for many accounts. This is why you should have a unique password for each account and change your password ASAP if you find out a platform you use has had a breach.

Signs your account has been hacked.

Does something seem off about one or more of your online accounts? Know the common symptoms of a hacked account.

1. Your social media profile publishes posts that you didn't create. Ditto for direct messages – hackers might use your account to send phishing DMs or posts to your followers. Often these posts encourage your friends to click on a link, download an app, or buy something through an online store.
2. Friends and followers tell you that they received emails from your email address that you never sent, or DMs through social media that you never authored.

3. A company tells you that your information was lost via a data breach. In many places around the world, companies are required by law to tell you if they lost your data in a breach or cyberattack.

What are 4 things to do when your account is hacked?

If you think an account is hacked, snap into action, and take a few quick steps to staunch the damage. You have the power to give cybercriminals the boot!

1. **Change the account's password.** This will likely lock out the hacker. Unfortunately, it can also work the other way around: the hacker might change the password and lock you out. In this case, try using the "forgot my password" function to reset it. If that doesn't work, contact the platform ASAP. If you used the same password for other accounts, you should change all of them, and start using unique passwords for every account. Use a password manager to generate and store all your passwords.
2. **Notify your contacts that your account was hacked.** Let them know they may receive spam messages that look like you sent them. Tell your contacts they shouldn't open these messages or click on any links contained in them. When the situation is cleared up, let everyone know that your accounts are secure again.
3. **Make sure your security software is up to date.** Scan your system for malware, especially if you suspect your computer might be infected with a virus. Antivirus software will scan your device to check for any security issues.
4. **Contact people who can help you.** If you suspect someone has stolen money, this might mean calling the police and your bank. If a work account was breached, let your IT department know. If a social media or email account was hacked, alert the platform, and seek their help. If you think someone has stolen your identity, it is worth contacting the FTC. Let trusted friends and family know what you are going through so they can on the lookout for weird messages or posts from your account.

How to protect your accounts from hacks.

As with most things in life, an ounce of cybersecurity prevention is worth a pound of cure. Follow our "Core 4" to show hackers you mean business.

1. Use long, complex, and unique passwords. Every password should be at least 12 characters long and include letters, numbers, and symbols (like % or $). Ideally, your passwords should be random strings of characters, not recognizable words. Very importantly, each account should be protected by its own unique password. To create and store all these passwords, use a password manager!
2. Switch on multi-factor authentication. Multi-factor authentication (MFA), sometimes called 2-factor authentication, adds a whole other level of security beyond your password. MFA will use biometrics, security keys, text messages, or an app to make sure you are you, even if a hacker gets access to your password. Enable MFA for any account that allows it!
3. Think before you click. Learn how to identify phishing messages, which will often try to inspire panic or urgency. Take a few seconds to read through the message and who sent it. With a little knowledge, you can spot most phishing attempts within moments.
4. Turn on automatic updates. The best way to get the latest, strongest security is to install software updates as soon as they are available – and the best way to know when they are available is to turn on automatic updates! Set it, forget it, and you won't regret it!

ADDITIONAL RESOURCES

Here's where to turn if you have an account with one of these popular websites and you think it's been hacked:

- eBay
- Facebook
- Google
- Instagram
- Outlook
- PayPal
- Snap
- TikTok
- Twitter
- Yahoo
- YouTube