

How to tell if you've been (or are about to be) hacked

Sometimes it's obvious that you've become a victim of a cybercrime. If you can't get on your network or your computer, you likely have a virus or you've been hacked. If your business receives an email from someone threatening to expose your personal information unless you pay a ransom, you're a victim of ransomware. However, not all cybercrimes are that obvious.

If you've been hacked, the sooner you find out and put a stop to the problem, the better off you'll be. To help you see potential signs, we've provided common ways to spot a scam or hack.



Your identity may have been stolen if:

- You see unusual activity in your bank account or credit card – like an unfamiliar charge, withdrawal, purchase, or even deposit
- Your bank or credit card statements stop showing up – either by mail or email
- You have good credit, but you've had an application for credit denied
- Statements show up for a credit card you didn't open
- A new credit card that you didn't apply for shows up in the mail



Your social media may have been hacked if:

- You can't log in to your account
- There are updates that you didn't post
- You have outgoing messages that you didn't send or create



You may be looking at a phishing email if it includes:

- Request for something unexpected, like a friend who needs money because they are "stranded" in a foreign country
- Urgency! Pressuring you to act quickly (without thinking it through)
- Poor grammar or misspellings
- Unrealistic threats or offers that are too good to be true
- Request for personal information
- A mismatched URL or misleading domain name

Want to learn more?

Contact your agent or broker for ideas on how to protect the online you – whether you're at home or at work – by preventing identity theft, phishing scams, and other cybercrimes before they happen. And find out what you can do if you're a victim of a cybercrime.

www.chubb.com/online-you-protected

Chubb. Insured.

