OUCH! November 2023

The Monthly Security Awareness Newsletter for You

I'm Hacked, Now What?

Have I Been Hacked?

The internet can be overwhelming, with new technologies changing all the time. No matter how safe you try to be, sooner or later you may be unfortunate enough to get hacked. The sooner you detect something bad has happened, and the faster you respond, the more you can minimize the impact. Below are signs that you may be hacked and if so, suggestions to resolve it.

Clues One of Your Online Accounts May Have Been Hacked

- Family or friends notify you they are receiving unusual messages or invites from you that you know you did not send.
- Your password to one of your accounts no longer works even though you know the password is correct.
- You receive notifications from websites that someone has logged into your account when you know you did not log in yourself.
- You receive emails confirming changes to your online profile that you did not make.

Clues Your Computer or Mobile Device Has Been Hacked

- Your antivirus program generates an alert that your system is infected. Make sure it is your anti-virus software generating the alert, and not a random pop-up window from a website trying to fool you into calling a number or installing something else. Not sure? Open your antivirus program to confirm if your computer is truly infected.
- While browsing the web, you are often redirected to pages you did not want to visit, or new pages appear unwanted.
- You get a pop-up window saying your computer has been encrypted and you must pay a ransom to get your files back.

Clues Your Credit Card or Finances Have Been Hacked

- There are suspicious or unknown charges to your credit card or unauthorized transfers in your bank account that you know you did not make.

Now What? – How To Take Back Control

If you suspect you have been hacked, stay calm. You will get through this. If the hack is work-related, do not try to fix the problem yourself. Instead, report it immediately. If it is a personal system or account that has been hacked, here are some steps you can take:

- **Recovering Your Online Accounts:** If you still have access to your account, log in from a trusted computer and reset your password with a new, unique and strong password - the longer the better. If you did not have Multi-Factor Authentication (MFA) enabled, now is a good time to enable it. If you no longer have access to your account, contact the website and inform them your account has been taken over. If you have any other accounts that share the same password as your hacked account, also change those passwords immediately.
- **Recovering Your Personal Computer or Device:** If your antivirus program is unable to fix an infected computer or you want to be surer your system is safe, consider reinstalling the operating system and rebuilding the computer. If you feel uncomfortable rebuilding, or if your computer or device is old, it may be time to purchase a new one.
- **Financial Impact:** For issues with your credit card or any financial accounts, call your bank or credit card company right away. The sooner you call them, the more likely you can recover your money. Don't call them using the phone number in an email, but use a trusted phone number, such as the one listed on the back of your bank card or their website. Monitor your statements and credit reports frequently. If possible, enable automated notifications whenever there is a charge or money transfer.

What to Do to Stay Ahead of Cyber Attackers?

OUCH Security Awareness newsletter is published monthly and has an entire series on how to secure yourself. In the Resources section below, we list the most important OUCH newsletters to read to protect yourself. These resources focus on three key steps:

1. Keep all your systems and devices updated and current to the latest version.
2. Use strong, unique passwords for each of your accounts, manage those accounts with a Password Manager, and enable MFA.
3. Be skeptical - keep an eye out for social engineering tactics such as phishing emails.

Guest Editor

Sarah Morales (@SarahManley) is a Senior Program Manager on Google's Privacy, Safety and Security team. She leads external engagement with a focus on building community, collaborations and partnerships. She is Wicys Board Member and actively engaged in DEI efforts within the cybersecurity community.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers
MFA: One Simple Step to Securing Your Accounts: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Emotional Triggers - How Cyber Attackers Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Phishing Attacks Are Getting Trickier: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/