The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Your Accounts
- Your Devices
- Your Information

Hacked: Now What?

GUEST EDITOR

Chad Tilbury is the guest editor for this issue. He has extensive experience investigating computer crimes and is a co-author of the FOR408 Windows Forensics and FOR508 Advanced Forensics and Incident Response classes at the SANS Institute. You can find him on Twitter as @chadtilbury, or on his blog, forensicmethods.com.

OVERVIEW

No matter how many steps you take to protect yourself or your information, there is still a chance you will get hacked. Like driving a car, no matter how safe you are, sooner or later you most likely will have an accident. However, you can still protect yourself, even after you have been compromised. The sooner you detect an incident, and the faster you respond to it, the greater chance you have of reducing the harm. To help you prepare, we discuss different ways to determine if your computers, accounts, or information have been compromised, and how you can best respond. For responding, most of our advice applies to your personal life. If you have a work related device, work account, or work information hacked, report the incident to your organization's help desk or security team immediately, and then follow their instructions.

YOUR ACCOUNTS

You probably have numerous online accounts for everything from online banking and shopping to email and social networking. Keeping track of them and identifying when an account is compromised can be a constant challenge. Here are some steps to help you identify and respond to compromised accounts.

Symptoms:

- You can no longer log in to the website, even though you know your password is correct.
- Your friends or co-workers are receiving emails from you -- emails that you never sent.
- Someone is posting messages on your social networking page (such as Facebook or Twitter), posing as you.
- Someone is transferring money out of your online bank account.
- Contact information or other settings on your online accounts are being changed without your knowledge or consent.
- A website or service provider publicly announces they have been hacked and user accounts or passwords have been compromised.

Hacked: Now What?

Response:

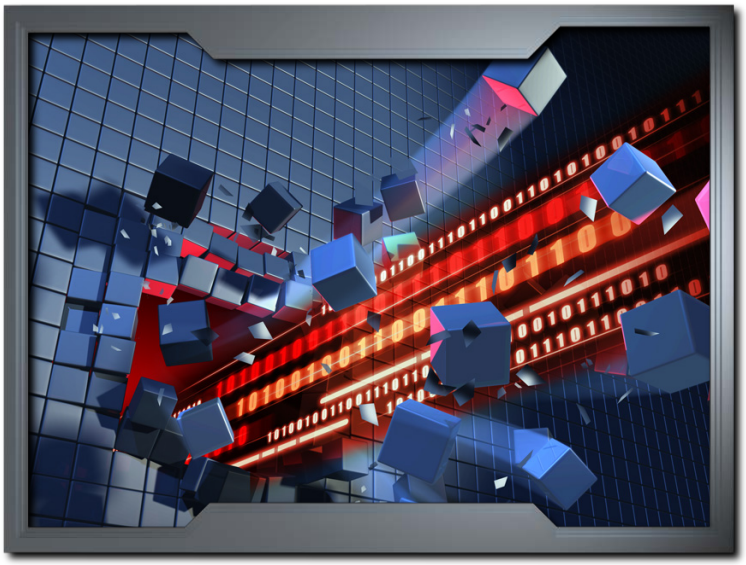
- If you can still log in, change your password immediately. As always, be sure to use strong passwords.
- If you can't log in, contact the service provider or website immediately. Most online providers provide some way to notify them that your account has been hacked. These methods can include an online form, an email address to contact, or a phone number to call.
- Once you have regained access, review all of your account settings to make sure nothing has been changed by the attacker.
- Make sure you change your password on any other accounts that have the same password.

YOUR DEVICES

With the explosion of mobile devices, we now have even more things to protect. Once attackers control your device, they have the ability to intercept every action you take on that device. Here are some steps to help you identify and respond to infected devices.

Symptoms

- Your computer is taking you to websites you do not want to go to.
- Your computer is running programs that you never installed.
- Your anti-virus reports an infected file.
- Anti-virus and system updates are failing.
- Your device is continually crashing.
- Your smart phone is making expensive calls or purchasing apps without your permission.



The sooner you identify you have been compromised and the faster you respond, the more you can minimize the harm.

Respond:

- Perform a full scan with your updated anti-virus solution. If it detects any infected files, follow the steps it recommends. You may want to consider running a secondary security scan from online scanners.
- If your device cannot be secured by your security software, or you want to ensure it is fully recovered, consider reinstalling the operating system or performing a full factory reset, installing the latest version of your anti-virus, and recovering your data from backup (you are doing regular backups of your personal data, correct?).

Hacked: Now What?

YOUR INFORMATION

Protecting your own information, such as your Social Security Number, medical history, or purchase history, is challenging, since you often do not control this data. Instead, organizations like your health care provider, your credit card company, or your school store and maintain this data. Here are some steps to help you identify when your personal information has been compromised and how to respond.

Symptoms

- A service provider announces or informs you they had an incident and your data may have been compromised, such as your credit card number or your medical history.
- You see unauthorized charges on your credit card.
- Your credit reports indicate loan applications you do not recognize.
- Your health insurance is processing claims for treatments you did not receive.
- You receive letters for overdue payments on accounts that you did not open.

Response

- Call your credit card issuer immediately. Have them cancel the credit card and issue a new one. This is a free service your credit card company should provide.
- Contact your service provider. For example, if you believe there is fraud with your insurance account or bank account, call your insurance company or bank.
- During any filing process, always document all conversations with date, time, and the name of the person you talked to. Keep copies of all written correspondence and use certified mail to show proof of delivery.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

How I Got Hacked:
http://preview.tinyurl.com/8q2jwsu

Free Online Security Scanners:
http://preview.tinyurl.com/9ky9s6w

Internet Crime Complaint Center:
http://www.ic3.gov/default.aspx

Identify Theft Resource Center:
http://www.idtheftcenter.org/

Facebook Hacked Page:
www.facebook.com/help/hacked

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org