Keep Your Business Safe

Helpful tips if your device or online accounts are hacked

A compromised computer or device could be disastrous for your organization if you aren't prepared. Here are some helpful tips to keep your business safe.

Isolate your device(s) and disconnect them from the internet
To sever the connection the hacker is using to access your computer and/or devices, you may need to disconnect from the internet. Unplug the network cable from your PC and turn off the Wi-Fi connection.

Many laptops have a switch to turn the Wi-Fi off. Don't rely on doing this through software, as the hacker's malware may tell you something is turned off when it's actually still connected. If you're using a smart phone or tablet, turn on airplane mode. Make sure your network and devices are secure and avoid using public computers or Wi-Fi hotspots. Isolating infected devices will prevent them from being used to attack other computers and can prevent the hacker from being able to obtain files and other information.

Scan Your Computer for Malware and Viruses
Scan your computer for any spyware, malware and viruses that may be stealing your account details or logging your keystrokes. Almost all malware is installed by victims themselves, often without them even realizing it. If there is something malicious on your device, it will need to be removed before you start the recovery process. Having a solid anti-virus product and running a security scan for malware and viruses is the most basic thing you can do. By using a brand-name commercial product that you pay for you can avoid installing additional malware. Many people who search for free antivirus actually end up installing additional malware. Malware antivirus software isn't perfect – they have a hit ratio of 50 to 75 percent and can miss almost as much as they find. Make sure you're running the most recent version of your operating system. It's important to keep your computer up to date on security patches, anti-virus and anti-spyware software, as well as having a good firewall in place.

Backup Your Important Files
Copy your photos, documents, media and other personal files to a DVD, CD or other storage device. Even if you think everything is clean, always scan your data files prior to reintroducing them back into your system.

If you still have doubts, contact your anti-virus software provider or a computer specialist
Be cautious when calling telephone numbers for technical support specialists that you find online. Scam artists sometimes set up authentic-looking websites that may appear to be affiliated with your computer's manufacturer. When consumers call these entities, they are often told they must pay hundreds of dollars for their computer to be fixed. The "technician" may also install additional malware or viruses onto your computer which will cause more problems. It's best to take the device to a physical repair shop, rather than trying to find a technician online. If you choose to call a technician online, be sure to research the company and its phone number to be sure it is legitimate.

Change all your passwords
After getting your devices repaired and all malware and viruses have been removed, you should consider changing all of your passwords. The malicious software that was removed from your computer may have transmitted your passwords to the attacker, granting them access to your accounts and personal information. This process is time consuming but very important! Hackers love the fact that many of us use the same logins for multiple accounts, so it's guaranteed they will try your info on sites like PayPal, Amazon and Netflix. It's possible that a hacker may also have changed your passwords, denying you access to your accounts. If you're unable to access your account, contact the providers directly and they'll help you restore your account. Your new passwords should be complex and totally unrelated to previous passwords, and you should never use the same password for multiple sites.

De-Authorize all apps and delete any sensitive data

One of the first things you should do if you've had an account compromise is de-authorize all associated apps that use that account for login. Google, Twitter, Facebook, Dropbox and others support OAuth, which enables third party apps to use your account without having to provide account login information. If a hacker has used it to authorize another device or service and remains logged in, simply changing your password won't get them out. There could be a rogue client out there you don't know about even after you regain access to your account. Your best bet is to pull the plug on everything you've given access to. It may be a pain to go back through and re-authorize them, but it's better than leaving a malicious individual lurking in your accounts. Any applications you're unfamiliar with or don't remember installing should be deleted. Delete any sensitive data stored in hacked accounts and any online auto-complete forms. Even if a hacker has access to your accounts, they may not have combed through all your data or files yet. If you're worried about any important files, especially those that contain personal information, delete them immediately. This is especially true for services like Dropbox, Google Drive and iCloud Drive.

Check for new accounts

If a hacker has access to your email, they may use it to set up new accounts. Check your inbox, sent items, and trash for any notifications that a new account has been created using your email address. If new accounts have been created, try logging into them by using the reset password feature and then deleting the account. If you have been hacked several times, consider getting a new one, but don't delete your current email address. Many experts warn against deleting email accounts because most email providers will recycle your old email address.

Be a detective: Ask yourself why

While you're fixing things, it's a good time to take a step back and ask yourself: What was the reason for the breach? If it was your bank account, the answer may be obvious. In other cases, like your email, it can be for several reasons – sending spam, requesting money or getting password resets on other services. An attacker may even be trying to gain access to your business. Knowing why you were targeted can help you understand how you were breached.

Notify and watch out for other users

Hackers often gain access to other accounts by using affiliated accounts since people are not as suspicious of emails coming from someone they know. When appropriate, contact your friends and family to tell them your device or accounts have been hacked. Notifying friends and family that your accounts have been hacked, and instructing them not to open urgent or strange emails, click on suspicious links or download attachments that seem to come from you may help protect their accounts from hackers. Scammers may even reach out to your contacts and say that you're in a different country and were robbed and need money. If your family and friends believe the emails are coming from you, they may try to send you money via Western Union, PayPal or some other service.

1-877-672-5678 | northwest.com

Where to report hacking

Hacking is a crime. You may file a report with the Federal Bureau of Investigation using the information below.

Federal Bureau of Investigation
Internet Crime Complaint Center (IC3)
The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Complaints can be reported to IC3 directly from their website: https://www.ic3.gov/

Otherwise, you can locate your regional FBI office, by visiting their website:
https://www.fbi.gov/contact-us/field-offices

You may also find additional information on consumer fraud, and file a report (complaint) with the Federal Trade Commission, and your state Attorney General's Office as follows:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue NW
Washington, DC 20580
(877) 382-4357
TTY: (866) 653-4261
www.consumer.ftc.gov

New York State Office of the Attorney General
The Capital
Albany, NY 12224
800-771-7755
www.ag.ny.gov

Ohio Office of Attorney General
30 E. Broad St., 14th Floor
Columbus, OH 43215
800-282-0515
www.ohioattorneygeneral.gov

Pennsylvania Office of Attorney General
Strawberry Square
Harrisburg, PA 17120
717-787-3391
www.attorneygeneral.gov

Protect yourself after a hack –
Scammers may try to use the stolen data to trick you into giving up more personal information.

- You might get letters in the mail saying you won something and provide a phone number to call to claim your winnings. Don't call it without thoroughly verifying the source. It may be a ploy to gather more information from you.
- Hang up the phone if you get a call asking for account numbers or other information.
- Don't click or respond to any texts from numbers you don't know.
- Don't open emails from unknown contacts or that look suspicious.
- Don't open attachments or click on links in social media messages you've received from unrecognized email senders – just delete them.
- Be wary of free downloads and website access, such as music, games, movies and adult sites. They may install harmful programs without you knowing.
- And finally, don't forget that hackers love social media – particularly those of us who overshare on it. So, before you post details of your adorable new kitten, remember it may just provide the perfect clue for a hacker trying to guess your email password!

Commit to multi-factor authentication

Multi-factor authentication adds another step to your login but it also adds another layer of protection. Enabling this will mean that in addition to your password, you will need a special one-time use code to login. This is usually sent to your mobile phone.

Use a password manager

Effective passwords are complicated, like Jov#UCB2yVJ6RkA, or icing-terminal-sconce-pizza. But they aren't easy to remember. Choose passwords and PINs that would be difficult for others to guess and update them regularly. Do not save them in plain text on your phone or computer. You may want to consider using a password manager application to create secure passwords without having to remember them. The only password you need to recall is a single, very secure password that lets you access all the passwords stored within your password manager.

Set up software to auto-update and run security scans

Some types of spyware can send keystrokes entered by a user to hackers who use it to pick up passwords and hack into online accounts. Anti-virus software is designed to detect these types of programs and remove them. Schedule routine antivirus security scans and software patch updates to run automatically.

Secure your wireless environment

Almost all computers and connected devices today are enabled for wireless and Wi-Fi communication, which can introduce security vulnerabilities as information flows over open frequencies to wireless connections to the Internet. Encryption algorithms scramble data and make it difficult for hackers to understand information they might intercept. Be cautious when using public Wi-Fi and encrypt wireless connections whenever possible.

Firewall Review

Your firewall may not be effectively protecting you. Firewalls can be very complex in nature to configure and maintain. Consider having an expert from a reputable company periodically review your firewall configuration to verify it's properly securing your connection to the Internet.

Northwest

1-877-672-5678 | northwest.com