You've Been Hacked! Seven Tips To Help Detect And Take Back Control

How do you know if your computer or mobile device has been the target of hackers?

PITTSBURGH, Jan. 24, 2018 -- The great heist movies of the past often featured villains as safecrackers, ammunitions experts or heavily armed individuals whose identities were masked by a simple handkerchief or ski mask. Oh, the good old days. Fast forward to villains today, known as hackers.

"Hackers today may be armed with nothing more than a computer, operating anonymously behind the scene using technology," said Deborah Guild, chief security officer of The PNC Financial Services Group. "While identifying the criminal is nearly impossible, individuals should be aware of the warning signs and learn what steps they can take to regain control of their device."

Hacking refers to the unauthorized infiltration of a computer or a network for illicit purposes. Phishing, SMiShing, ransom ware and malware and skimming are all different and common methods used to hack a system or system data.

Tips for Detection

So how do you know if you may have been hacked, and what can you do about it? Some signs that you may have been hacked, include:

1. **Your password is no longer working**. Before hitting the panic button, verify that the website itself is not having a technical issue that could impact your logon.
2. **New programs appear unexpectedly on your computer.** These programs may be found listed in your "Start Up" menu or found on the desktop, but you did not install them.
3. **Your anti malware program is disabled.**
4. **You identify unauthorized transactions on your bank account or credit cards.**
5. **Your system is excessively slow**.
6. **Friends report unusual emails sent from your account** – However, you did not send them; you are not the true sender.
7. **Your computer is active during the night.** If your computer should be in sleep mode when you are, but instead you find it to be active when you go for that midnight snack, a hacker could be involved.

All of these signs individually could be symptoms of other technology issues. But when troubleshooting, keep in mind the potential that the device may be compromised.

Tips for Taking Back Control

If you suspect that your computer has been compromised by a hacker, some steps that may help towards recovery include:

1. **Download the latest anti-virus product from a reputable source and scan your computer for malware and viruses** – Detecting and eliminating malware is a first step in recovery. This is not a cure-all, but a good start.

2. **Reset all of your online passwords** – Change your passwords from a different device, one that you are confident has not been hacked. Some post-hack malware can alert the hacker of activity on the keyboard of the compromised device and can even capture your new passwords to share with the bad actors.
3. **Reset the Personal Identification Number (PIN) for your accounts**- Similar to password changes, use a device you are confident has not been hacked to change PINs associated with each account.
4. **Contact your bank** – If you used the compromised computer or device for banking purposes, contact your financial institution immediately to review account activity to identify potential fraudulent transactions or unauthorized changes to your account.
5. **Contact credit/debit card companies** – If you used the device to make purchases with credit or debit cards, contact the card issuer using the phone number on the back of your plastic card to see about restricting access to your accounts or to close accounts and open new ones if necessary. Continue to monitor your bank and credit card accounts for unauthorized activity, and report it immediately.
6. **Use a backup to restore your computer to a date prior to the suspected hacking.**You risk losing data added after the last backup occurred; however, it is preferable to losing more to a hacker.
7. **Check settings on your accounts** - Make sure that there is no forward on the email address or other changes.

Tips for Protection

Help to defend against intruders in your computer system with some basic best practices:

- **Be diligent in keeping your devices up to date.** Many hardware and software manufacturers routinely publish updates meant to strengthen your security and protect from emerging threats. Everything from your home computer to your phone, to even your Wi-Fi router need to be periodically upgraded by the manufacturer. While some devices, like your phone, can be set to do this automatically, others cannot. Be sure to consult all appropriate owner's manuals and upgrade all devices as appropriate.
- **Set up alerts on your accounts** – Ask your financial institution about setting up alerts so they can contact you when the contact information or alert choices for the account are requested. Such alerts can help to verify that you, the account owner and not a hacker, are requesting the changes. You also can set up transaction alerts to easily help keep an eye on purchases made from your account.
- **Back up your computer regularly** – At minimum, you can restore your computer back to the way it was before it was hacked.

For more information about prevention and detection, visit PNC's Security and Privacy website.

The PNC Financial Services Group, Inc. (NYSE: PNC) is one of the largest diversified financial services institutions in the United States, organized around its customers and communities for strong relationships and local delivery of retail and business banking including a full range of lending products; specialized services for corporations and government entities, including corporate banking, real estate finance and asset-based lending; wealth management and asset management. For information about PNC, visit www.pnc.com.

CONTACT:

Amy Vargo
(412) 762-1535
amy.vargo@pnc.com

Additional assets available online: Photos (1)

https://pnc.mediaroom.com/2018-01-24-Youve-Been-Hacked-Seven-Tips-To-Help-Detect-And-Take-Back-Control