CYBER SECURITY
Newsletter

HACKED … NOW WHAT?

Problem

Using computers on the Internet is like driving a car -- you take steps to protect yourself but an accident can happen at any time. With computers and the Internet it is the same. You take the proper steps to protect yourself, but your computer or your personal information may be hacked. You are often not in control of your own data; other companies or organizations control it. Retail stores record your purchases, your mobile company tracks your phone calls, and your doctor stores your medical records. Not only do you have to worry about protecting your own data, you have to worry about others protecting your data.

Solution

The key to protecting yourself is detecting and responding to an incident as soon as possible. If you notice something is wrong and react quickly, you can save yourself and our organization a great deal of time and trouble. To help protect you, we will cover the three most common ways to detect if your data or your computer has been hacked and how to respond.

1. Login Accounts

One of the first places you may detect a problem is with your login accounts, such as your online banking, work email, or any resource that requires a login and password. The first indication you may be hacked is when you can no longer log in and your password does not work. If you know you are using the correct login and password, but your log in attempts keep failing, a cyber attacker may have hacked into your account and changed your password.

If your password fails on a work account, contact the help desk or information security immediately. The sooner you contact them, the faster they can respond and stop the attacker. If it is not a work related account, contact the administrators of the website. Every website should have a contact email address or phone number. If you believe your password has been hacked, check to see if you are using the same password on any other accounts. If you are using the same password, change them immediately.

You Have Been Hacked

At some point, you may find your computer or your information compromised. The faster you respond, the less damage the attackers can do.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

© The SANS Institute 2012

Your Security Team

Our organization has a highly trained security team dedicated to helping protect you. These professionals are experts who understand cyber criminals, specifically how they attack and what to do to protect against them. This team has helped design and deploy many of the technologies we are using, including anti-virus and firewalls. Our team is constantly monitoring our networks and looking for the latest attacks on our organization.

However, our security team cannot always guard everything. We need your help in protecting our organization. One way you can help our security team is to alert them if you think you see an infected computer. It is often employees like you that are the first to see or find something wrong. Our security team will be happy to hear from you, they know you are trying to help.

2. Your Financial Accounts

One of the primary goals of cyber criminals is to gain control of your financial accounts. The easiest way for them to make money is to steal your money. The primary way they do this is to steal your login and password to your financial accounts. They may do this through phishing attacks, infecting your computer, or using the same login and password you use for other accounts. Once they obtain your account information, they then use it to buy items or transfer your money to their accounts.

The simplest way to detect if your financial accounts have been hacked is to monitor your monthly statements. If you see a charge or withdraw you did not make, immediately call your bank. Your bank contact information can be located on their website, your banking card (if you have one), or in your monthly statement. If your bank account has been compromised, your bank will ask you to change your online password and ATM PIN. They will then issue a new banking card.

3. Your Computer

Your computer is a primary target for many criminals. Unfortunately, determining if your computer is hacked is not as easy as it may seem. When computers are hacked, they often perform slowly, crash frequently, or may even reboot. How can you tell if your computer is hacked or just acting up?

One way you can tell is through your anti-virus program. Your anti-virus software should scan your computer every time you save, open or run a file. If it finds a virus on your system, your computer may have been hacked. To ensure your anti-virus is effective, make sure you update it every day (it should do this automatically). If anti-virus reports your work computer is infected, report it immediately. If this is not a work related computer, then have the anti-virus program clean and fix your computer. In addition, change all your passwords, as cyber criminals may have captured them.

Another way to tell if your computer is infected is when your computer redirects you to websites you do not want to go to, such as gambling sites, medical drugs, or pornography. This is known as spyware. Cyber criminals make money by re-directing you to websites they control or websites that pay cyber criminals for people to visit them. Once again, if you are concerned your work computer is hacked, report it immediately.

© The SANS Institute 2012