

# Hacked! Now What?



## Enterprise Information Security Office

### Monthly Security Tips Newsletter

*From the Desk of Deborah A. Snyder, Acting Chief Information Security Officer*

Maybe you opened an email attachment you shouldn't have and now your computer has slowed to a crawl and other strange things are happening. Or perhaps you're running an out-of-date, or unpatched, operating system software (such as Windows XP) and have started to see "antivirus warnings." Perhaps your bank called informing you that there has been some unusual activity on your account. Your friends and family may start complaining about spam messages they are purportedly receiving from you. These are all signs that your computer may have been hacked.

If your computer system has indeed been compromised and infected with a virus or other malware, you need to take action to protect your data and prevent your computer from being used to attack others.

#### **Secure Your Computer**

Ensure your computer is current with all available patches, fixes, and upgrades. If you do not have your operating system set to automatically update, do so now by visiting your operating system's website and following the instructions. Links are provided here for [Windows](#) users and [Mac](#) users. **(In addition, note that support for Windows XP ended effective April 8, 2014. The end of support for Windows XP means that Microsoft will no longer provide new security updates and will therefore become a significant security risk. It is recommended that anyone using Windows XP migrates to products that are supported, such as Windows Vista, Windows 7 or 8.)**

Your computer's security software should also be up-to-date. To check status, click on the icon for the security program on your system. If an update is needed, it will be indicated here. If you don't have security software installed, you need to get it. Make sure you have anti-virus and anti-spyware software installed and a firewall enabled.

Confirm that your browsers are up-to-date. Tools such as [Qualys BrowserCheck](#) or [WhatBrowser](#) can help assess status.

#### **Secure Your Accounts**

You probably access numerous online accounts, including social media, banking, news sites, shopping, and others. If you've been hacked, there is a chance that important passwords have been stolen. Reset your passwords for your critical accounts first, starting with your email account, followed by financial and other critical accounts. It is important to start with email accounts, since password resets for all of your other accounts are typically sent to your email.

Use separate and unique ID/password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters, and by changing them on a regular basis. If you are unable to log into one of your accounts, contact the service provider or website immediately. Most online providers include an online form, an email address to contact, or a phone number to call.

## Secure Your Mobile Device

Our increased reliance on smart devices—including mobile phones and tablets—for everyday activities has resulted in an increased number of hacking attempts against these devices. As we do with our personal computers, we have to ensure the proper steps are taken to protect our information and devices. This includes installing security software, where available, and keeping all installed software up-to-date.

### For More Information

---

**Office of Information Technology Services Enterprise Information Security Office –**  
<http://www.its.ny.gov/eiso>

You've been hacked, now what?  
<http://www.net-security.org/article.php?id=1827>

Provided By:



*The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

*Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.*