Internet Safety: How to Protect Yourself Against Hackers

From the Office of Minnesota Attorney General Lori Swanson

Some criminals, known as hackers, illegally obtain usernames and passwords from websites, making those with an online account vulnerable. Many people shop, bank, and pay bills online, presenting hackers with opportunities to access their personal and financial information. Hackers, generally located outside the United States, are difficult to stop because they use cutting edge technology to evade law enforcement and acquire large amounts of information, often undetected.

There are two main ways hackers may try to get your personal information. One way is to try to access information directly from your computer by installing spyware. Spyware is software that installs itself and sends information from your computer to others without your knowledge or consent. Hackers install spyware by tricking you into opening spam email, or by "clicking" on attachments, images, and links in email messages, instant messages, and pop-up messages. Hackers use spyware to track keystrokes or acquire pictures of your computer's monitor in the hope of snagging account numbers, passwords, and other sensitive information.

Hackers also may access sensitive information directly from websites. Any website that has personal or financial information may be vulnerable. Hackers use malicious software, or "malware" to target websites, gathering massive amounts of information. Malware is used to infiltrate computers in order to steal private information or harm the operation of the computer system or its security. Malware allows hackers to test a website's vulnerability and reproduce the contents of the website's database. The database contains security information that allows hackers to access individual accounts.

If Your Online Accounts are Hacked

- ✓ You may not be immediately aware that an online account has been hacked. If friends or family members contact you about emails that seem like they are from you but which you did not send, it is generally due to your account being hacked. A hacker may also change your password, denying you access to the account. If one of your accounts has been hacked, change your password immediately. If you are unable to access your account, contact the website directly and it can assist you in restoring your account.
- ✓ Contact your friends and family and make them aware your account has been hacked. Hackers may try to gain access to your email contact list, and send emails from your account. Notifying friends and family that your account has been hacked may help protect their accounts from hackers.
- ✓ If the hacked account contains financial information, contact your bank or credit card company immediately, letting it know that your account may be compromised. Your bank or credit card company may issue you a new card or account number. Be sure to monitor activity on the account for any fraudulent transactions. In some cases, hackers may have obtained your information, but will not use it right away. If you are not issued a new card or account number, you should monitor your account for an extended period.

Protect Yourself

Update your computer security

Make sure your security software is up to date. The operating systems of personal computers and the Internet-connected software (like email programs, web browsers, and music players) should be updated regularly. If you do not have security software already, install a firewall and antivirus software and keep them up to date. Your computer will notify you when an update of the software is available. You will also want to install anti-spyware/malware software. There are a variety of reputable products available for free or that have a free trial period. Do your research before installing any program and beware of scams that attempt to lure you into disclosing your personal banking information or that direct you to download programs that may contain malware with the ability to drain private bank account information from your computer.

Know your activity

It is best to delete spam or dubious looking emails without opening them. If you receive a questionable email from a friend or family member, it is best to contact them and verify they were the sender before opening the email or clicking on a link or attachment. If possible, only access online accounts from your personal computer while using a secured Internet connection.

Try to limit accessing personal accounts from public computers that could be infected with spyware/malware or may have an unsecured Internet connection. If you do use public computers, be sure to log out when you are finished.

Password protection

To reduce the chances of your online accounts being hacked, change your passwords frequently. Strong passwords are at least 12 characters long, include numbers, letters, special characters (&,!,?, etc.), and are not too predictable. For example, don't use your name or date of birth for your password or use common words like "password." If you have multiple online accounts, it is best to have a different password for each account. In the event that one of your accounts is hacked, having different passwords for your other accounts reduces the likelihood of those accounts being accessed.

Storing information

Many websites now store personal banking information to make it easier for you to buy a product or to pay a bill. Although convenient, in the event that your account was hacked, your banking information would be more easily available to hackers. Ensure any website with banking information is secure, that your password is unique to that account, and that you log out once you are done.

Reporting Hacking

Hacking is a crime. You may file a report with the Federal Bureau of Investigation, which may be contacted as follows:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
763-569-8000

You may also wish to file a report with the Federal Trade Commission as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
Toll-free helpline: 877-382-4357

For more information on consumer issues, contact the Minnesota Attorney General's Office as follows:

Office of Minnesota Attorney General
Lori Swanson
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
651-296-3353 or 800-657-3787
TTY: 651-297-7206 or 800-366-4812
www.ag.state.mn.us