Internet Safety:

How to Protect Yourself Against Hackers

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity and respect

Recent reports estimate that there will be between 20 and 30 billion Internet-connected devices by 2020. Many people are familiar with computers, tablets, smartphones, and wireless Internet. Now other "smart" devices, like televisions, home security cameras, and even refrigerators, connect to the Internet. More devices mean more avenues for attack by hackers.

What is Hacking?

Hackers illegally access devices or websites to steal peoples' personal information, which they use to commit the crimes like theft. Many people shop, bank, and pay bills online. People also store financial information, like credit card or bank account numbers, on their devices. A hacker can do a lot of damage even if only one account or device is compromised. To make matters worse, hackers are difficult to stop because they are often located outside the United States and use cutting edge technology to evade law enforcement and acquire large amounts of information.

There are two main ways hackers may try to get your personal information. One way is to try to obtain information directly from an Internet-connected device by installing spyware, which sends information from your device to others without your knowledge or consent. Hackers may install spyware by tricking you into opening spam email, or into "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 device's screen in the hope of snagging account numbers, passwords, and other sensitive information. Criminals can also hack individual websites—like email, social media, or financial institutions—and steal the information stored there.

While trying to protect all your devices and accounts from these criminals may seem daunting, there are some easy, practical steps you can take to keep your information more secure.

Protecting Computers and Laptops

- **Make sure your security software is up-to-date.** Devices' operating systems and Internet-connected software (like email programs, web browsers, and music players) should be updated regularly. Your computer will typically notify you when a software update is available.
- **Install antivirus and antimalware software.** If you do not have security software, install a firewall and antivirus software and keep them up-to-date. There are a variety of reputable products available for free or that have a free trial period. These programs help identify the latest threats and allow a user to remove malicious software from their device. Do your research before installing any program and beware of scams that attempt to lure you into disclosing your personal information or that direct you to download programs that may contain malware.
- **Disable connections when you aren't using them.** If your computer uses Wi-Fi or Bluetooth to connect to the Internet and other devices, you should turn these features off when you aren't using them. This can prevent unknown persons from using your network or accessing your devices without your knowledge.

Protecting Cell Phones

- **Create a strong PIN or passcode.** If your device is lost or stolen, a strong passcode may prevent a thief from accessing all the information stored on your phone. Many smartphones also allow you to remotely wipe the information from your computer in the event of loss or theft.

- **Only install trusted applications.** Some criminals make available applications (or "apps") that look and function like legitimate apps, but actually install malware to your smartphone. Be sure to download apps only from trusted sources, and check the number of downloads and read reviews to makes sure you aren't downloading a "lookalike" app.
- **Keep your software up-to-date.** Smartphone manufacturers and app developers regularly release software updates that often include security improvements. Check often to ensure that your smartphone has the most up-to-date software.

Protecting Other Internet-Connected Devices

As mentioned above, Internet-connected televisions and appliances are now available in the marketplace. These devices, as well as the router that connects your home to the Internet, are also vulnerable to attack. It is important to protect these devices just like computers and smartphones.

- **Review your network and device names.** Is your cell phone or home network named using your last name or other personally identifying information? This can make your device more vulnerable to attack, since it connects the device to you and makes it easier for hackers to guess your password. You should change the name of your devices and network so hackers cannot identify you so easily.
- **Create unique passwords for all devices.** When you purchase a new device, it often comes with a simple, default password. Many people set up unique passwords for their computer or phone, but neglect to do so for their Internet router or other smart device. Unknown to the user, hackers can easily gain access to these devices, and use them to flood websites with so much traffic the site goes down or hack into your network. If, for example, your "smart" kitchen stove is connected to the Internet and has a simple password, a hacker could use the stove to access your wireless network and hack your computer or phone. When you get a new Internet-connected device, you should be sure to create a strong, unique password for it.

Protecting Online Accounts

- **Delete suspicious emails.** 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 that person and verify he or she sent it before opening the email or clicking on a link or attachment.
- **Use secure devices.** If possible, only access online accounts from your personal computer, tablet, or smartphone while using a secured Internet connection. Try to limit accessing personal accounts from public computers that could be infected with spyware or malware, or may use an unsecured Internet connection. If you do use public computers, be sure to log out when you are finished. In general, it is more secure to use a smartphone's cellular data network than a public or unsecured Internet connection.
- **Create strong passwords.** 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 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 too.
- **Use multifactor authentication on your accounts.** Multifactor authentication works like this: When you enter your password for your email account, for example, you are directed to a page that asks for a four-digit code. Your email provider then sends a unique, temporary code in a text message or to another email account. You must enter the code, which expires after a short amount of time, to access your account. This means that hackers who obtained your password still can't access your account unless they also have access to that verification code, adding another layer of protection. Many email providers, social media

websites, and financial institutions now make it easy for users to set up multifactor authentication on their accounts.

- **Be cautious with "Save my information for next time."** Many websites now store personal banking or credit card information to make it easier for you to buy a product or to pay a bill in the future. Although convenient, if your account is hacked, your payment information is more easily available to hackers. Ensure any website where you enter your financial information is secure (the website's URL should start with "https://"—remember that the "s" is for "secure"), that your password is unique to that account, and that you log out once you are done.

- **Sign up for account alerts.** Many email providers and social media websites allow users to sign up for an email or text alert when your account is accessed from a new device or unusual location. These email or text alerts can quickly notify you when an unauthorized person accesses your account and can help minimize the amount of time an unauthorized user has access to your information. If you receive such an alert, login to your account immediately and change the password. Check these emails closely, however, since malicious "phishing" emails often mimic these kinds of alerts.

If Your Device or Online Accounts are Hacked

- **Have devices inspected.** If your computer or other device is hacked, disconnect it from the Internet and have it looked at and repaired by a trusted 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, or the "technician" installs other viruses onto the computer that steal information or cause more problems. It is often best to take the device to a physical repair shop, rather than trying to find a technician online. If you call a technician online, be sure to research the company and its phone number to be sure it is legitimate.

- **Change your passwords.** After getting a device repaired or cleaned of viruses, you should change all the passwords for any accounts you accessed using the device. The malicious software that was removed from your computer may have transmitted your passwords to an attacker, granting the hacker easy access to your information. Similarly, if one of your online accounts has been hacked, be sure to change your password immediately. A hacker may also change your password, denying you access to the account. If you are unable to access your account, contact the website directly and it can assist you in restoring your account.

- **Monitor financial accounts.** If a 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.

- **Notify others.** When appropriate, contact your friends and family and make them aware your device or 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, 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.

- **Watch out for other users.** People often are not immediately aware that their email or social media accounts have been hacked. In fact, many people only learn of the problem when friends or family contact them about a suspicious email or message

from their account. If something doesn't seem right about a person's email or social media account, it is possible the account was hacked. Do not respond to any emails or messages you receive, but contact your friend or family member directly and tell them about the problem.

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
www.fbi.gov

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
(877) 382-4357
TTY: (866) 653-4261
www.consumer.ftc.gov

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

Office of Minnesota Attorney General
Keith Ellison
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
www.ag.state.mn.us