Ohio Attorney General's
Consumer Advocate
Newsletter
SEPTEMBER 2015

Five Tips to Shut out Hackers and Malware

Whether you're shopping online, connecting through social media, or checking web-based email accounts, take steps to protect your personal information from hackers and malicious software, also known as malware. Hackers often use malware to gain unauthorized access to users' Internet-connected devices, which can include personal information.

Examples of malware include viruses and spyware. Viruses are programs designed to infect computers and spread to other users' devices. For example, a virus may stop your computer's operating system from loading. Spyware may track and steal your personal information, such as passwords and credit card numbers.

Follow these tips to help keep your network and personal information safe:

- Don't leave your home-wireless network unsecured. An unsecured network may give intruders easy access. Ensure the Internet connection is behind a firewall. A firewall refers to either hardware or software that controls the information entering and exiting the network. Firewalls help keep would-be intruders off your network, making it harder for them to capture your personal information.
- Choose complex passwords for your wireless router and network connections. This will prevent strangers from being able to access your network.
- When available, always choose to enable encryption. This will scramble data into an unreadable format for anyone trying to view your network from outside.
- Run antivirus software updates regularly, or opt to have your devices automatically update once new versions become available. Cybercriminals regularly launch new viruses, so these updates are important. Software should be set up to scan the device on a regular basis. Also, update the computer's operating system and Internet browser, since those updates may contain new security patches.
- Never click on suspicious links, attachments, or pop-up advertisements, and don't trust someone who calls you unexpectedly to report a problem with your computer. Scammers often use these tactics to trick consumers into clicking on links designed to activate malware.

Visit www.staysafeonline.org for additional tips and a list of websites offering free "security check ups" to examine your computer for malware.

Contact your Internet service provider and the manufacturers of your computer and wireless router for more information about how to improve your network's security. A simple Internet search also may help you understand how to secure your network.

While setting up a protected network is very important, it is only a small step toward staying safe in cyberspace. Stay tuned for the next *Consumer Advocate* for another article about protecting personal information online.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.

Ohio High School Students: Enter the Attorney General's Scholarship Contest!

Are you looking for ways to earn money for college? Do you enjoy shooting and editing short videos? If so, put your consumer knowledge and creativity to the test by entering the seventh-annual Take Action Video Contest.

The top three winning individuals or teams will receive college scholarships of $2,500, $1,500, and $1,000, respectively, and may be featured on the Attorney General's website.

To enter the contest, Ohio high school students (grades 9 to 12) must produce and submit a 60-second informational video on one of the following topics:

- Identity theft
- Cybersecurity
- Student loans

The deadline to submit a video is Dec. 11, 2015. Winners will be announced in March 2016 during National Consumer Protection Week.

Visit www.OhioAttorneyGeneral.gov/TakeActionContest to view last year's winning videos, the official guidelines, and the 2015 Take Action Contest flier. Teachers are encouraged to print out and display a copy of the flier in their schools.

Contest questions should be directed to ConsumerOutreach@OhioAttorneyGeneral.gov.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.

Fake Check Scams Target Ohioans

Imagine selling an item online and then receiving a check for more than the agreed price. Would you deposit the check into your bank account and send the excess money back to the buyer? If so, beware! Scammers are using variations of the "fake check scam" to trick consumers into sending money using wire-transferring services and prepaid money cards.

How the Scam Works

A scammer poses as an interested buyer for a product that a potential victim advertises online. After expressing interest, the scammer sends a legitimate-looking check for more than the agreed-upon price of the product. For example, the scammer may send a check for $2,000 more than the selling price and say the remainder should be used to pay a "shipping agent." The scammer asks the victim to deposit the check and buy a prepaid money card or use a wire-transferring service to send the difference to the "agent."

In reality, the check is counterfeit, and the funds will not clear the bank even if the bank provides the victim with temporary access to those funds. Later, after the victim sends money to the "agent," the bank informs the victim that the check was fraudulent and that no money was deposited into the victim's bank account. Any money sent using a wire-transferring service or prepaid money card will be lost. In some cases, the bank may also charge a fee for depositing a bad check or for overdrawing an account.

Recently, a Pickaway County consumer reported being contacted by a potential "buyer" for his $1,000 telescope advertised online. The "buyer" planned to send a certified check for $3,000 and instructed the potential victim to deposit the money and withdraw $2,000 to send to "movers." Fortunately, the consumer reported this scam to the Ohio Attorney General's Office before losing any money.

Tips to Avoid Scams

If you post items for sale online, watch for signs of a scam, including:

- Buyers who say they can only pay by personal or cashier's check.
- Buyers who send you a check for more than the asking price.
- Pressure to return any overpayment immediately.
- Requests for wire-transfers, money orders, or prepaid money cards. These are the preferred methods of payment for scammers, because they are nonrefundable and difficult to trace.
- Buyers who want the products or excess money to be sent to someone else.

Beware of other variations of the fake check scam, including those based on a phony mystery shopper assignment, fake job opportunity, or fraudulent sweepstakes. In these scenarios, victims may be asked to send money to "evaluate their local wire-transferring service" or to "cover fees associated with their winnings." In reality, any money sent will likely be lost.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.

What to Know About Debt Collection Calls

When dealing with a debt collector, it is important to understand your rights and to distinguish between a legitimate debt collector, a debt collector who fails to comply with the law, and a likely scam artist.

Knowing what debt collectors can and cannot do under the law will help you avoid fraud.

Laws concerning debt collection are found in the federal Fair Debt Collection Practices Act (FDCPA). The FDCPA specifically covers personal debts being collected by a third-party collector (not the original creditor). Money owed on personal credit cards, auto loans, medical bills, and mortgages are all examples of debts covered by the FDCPA.

Under the law, debt collectors may use phone calls, letters, email, or text messages to attempt to collect a debt, but they cannot:

- Contact consumers before 8 a.m. and after 9 p.m., unless the consumer approves the calls outside these times.
- Contact a consumer at work if they have been told the consumer is not allowed to receive the calls there.
- Pretend to be attorneys or impersonate representatives of a government agency if this is not true.
- Provide information about a debt to anyone but the debtor, an attorney representing the debtor in the matter, or the spouse of the debtor.
- Harass, threaten, or deceive debtors.

While debt collectors are prohibited from certain acts, they must:

- Identify themselves when contacting the debtor.
- Stop contacting consumers who request to not be contacted. A consumer who wants to prevent any further contact from a collector can send a letter to the collector requesting the communication to

end. The collector must then cease contact, with the exception of acknowledging that there will be no further contact or notification that the collector intends to file a lawsuit or take other action. However, this will not get rid of the debt.

- Send a letter within five days after the initial phone contact that includes the amount owed, to whom it is owed, and how long a consumer has to dispute the debt. Within 30 days of receiving the notification, a consumer can dispute a debt and request verification of the debt by sending a letter to the collector stating that a portion or the full amount of the debt is not owed.

Although there are many legitimate debt collectors, some "collectors" are scam artists who try to intimidate consumers into sending money or revealing personal information. They often threaten to arrest someone if a debt is not paid immediately. They also may threaten to seize property or garnish wages. Scammers tend to create a sense of urgency but refuse to provide any documentation of the debt. They also will ask for payment using wire-transfers or prepaid money cards.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.