Brian E. Frosh
Attorney General

Media Contacts:
Press@oag.state.md.us
410-576-7009

Consumer Alert

Consumer Alert: Cyberthieves Are Posing as Major Companies in Phishing Schemes

Have you received an unexpected or unsolicited email, phone call, or text from a major company like Amazon, Google, or Apple? Before you click on the email or respond to a text or phone call, know that it's probably a scam. These types of scams are on the rise, and scammers are trying harder than ever to trap victims, and they are becoming more aggressive.

Often, these emails/calls/texts will state something like:

- Your account has unusual/suspicious activity;
- Your account has been altered and needs your attention right away;
- You need to update your payment information; or
- You need to take some other action, usually "urgently."

Other times, you may receive what looks like an order confirmation, that may or may not include an attachment, for an item you didn't purchase.

A scam email or text will often ask you to click a link, open an attachment, or call a number to resolve whatever issue it says needs your attention. When people respond, they're often asked to purchase gift cards or visit a website (provided by the scammer) to input payment information to resolve the issue. But to be absolutely clear— you should never call any number, open any attachments, or visit any website one of these calls or emails tells you to. This is one of the most common ways these scammers can trap you. The link could send you to a malicious website or launch a virus into your computer or phone. Alternatively, it may ask you to "verify" or submit personal or financial information, but the scammers are really just stealing it.

If you get a phone call from a representative claiming to be from one of these major companies, please be aware that they will rarely call you for any reason. Our advice is to ignore these calls, or if you do pick up and the caller asks you to disclose or verify personal and financial information, hang up right away. Major companies like Amazon, Apple, and Google will not ask you for this information unless you have initiated the call. If your phone service allows it, you may wish to block the suspicious caller's number.

There are red flags that can tip you off that you're dealing with a scam email or text. It could contain poor grammar and/or spelling, or the content just seems strange or farfetched. If the email originated from a different account than the supposed company trying to contact you (for example, an email claiming to be from Apple would not have a sender email address ending in gmail.com), it may be fraudulent. Is the link embedded in an email actually the same as the text

that is displayed? For instance, if the link says www.amazon.com, but displays something completely different when you hover your cursor over it, it may be fraudulent. Finally, if you didn't sign up for text messages or alerts from a particular company, you should ask yourself why they would contact you that way.

If you do need to contact a company's customer support, go directly to the company's official website to see how they prefer you contact them.

If you do provide information or purchase gift cards at the request of these scammers, recovering your money will be very difficult. Remember, providing personal information also makes you vulnerable to identity theft. If you believe the scam may have originated in the United States, we recommend that you contact your local police department or State's Attorney's Office to determine if they can assist you in recovering any of your money.

If you believe this scam may have originated outside of the United States, we recommend that you contact the FBI at www.fbi.gov to determine if they can assist you in recovering any of your money. Alternatively, you may call the Baltimore office at 410-265-8080 or the National Headquarters in DC at 202-324-3000. This type of crime may also be reported to the Internet Crime Complaint Center at www.ic3.gov.

The best way to protect yourself from these types of scams is to know the red flags and trust your instinct if you suspect something is off. Don't answer suspicious calls, but if you do and suspect it's a scammer—hang up and block the caller's phone number. Delete suspicious emails and texts. If you do open them, do not click on any links, open any attachments, or call any of the numbers listed. You are your own best defense against these scams.