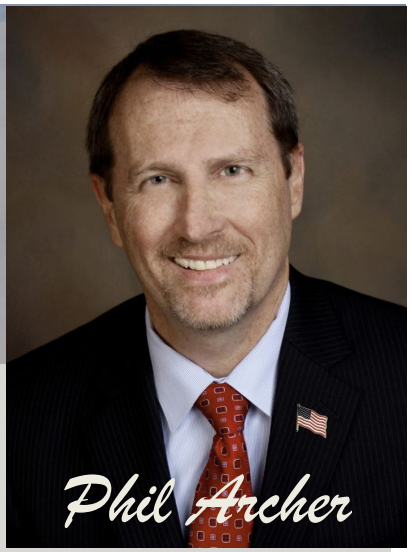
Phil Archer
State Attorney
18th Judicial Circuit
Brevard and Seminole County
Domestic Violence Awareness Month



The Monthly Brief

Volume 8 Issue 10 October 2020

Google Photos Scam

You get an email or text message that appears to come from Google Photo. Someone is sharing an album of photos with you. To view the photos, you just need to click the link. The message looks so real! It may use a convincing URL, which has been created by Google's goo.gl URL shortener to appear to be an official Google domain name. The message also seems to come from noreply-photos@google.com.

The catch? There is no photo album. It's a phishing con. When you click the "View Photo" link, it will open in your web browser and prompt you to log into your Google account. If you enter your information, you are giving scammers your username and password. Con artists can now access your email account as well as any other accounts that use the same login information.

Tips to Avoid These Types of Scams

Never click on links in unsolicited emails or text messages, especially if you don't know and trust the person who sent it.

Be careful with shortened links. such as Bit.ly or Goo.gl, because you often can't tell where the link will take you.

Be careful of any message that comes from a friend but seems out of character. It may have originated from their account, but they could be victims, too.

Don't fall for "urgent" scams. Scammers like to cause alarm to create urgency so you'll act without thinking first. You might get a message that indicates a dire situation that needs immediate attention. If it seems unlikely, watch out. Source *BBB. org

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Holiday Delivery Scams

Some consumers have recently been getting text messages that say a major delivery carrier needs them to "update delivery preferences" on a package by clicking on a link. The problem? The text is a scam, and the link results in theft of personal information.

Particularly prevalent at the holidays, these scams can happen year round. Scammers are hoping shoppers are busy or distracted and will act without thinking.

The first scam to look out for are phishing texts or emails that pose as official notices from delivery companies. These either contain a "tracking link" or a message that the shipper is having difficulty delivering a package to you, or most recently, a link to update delivery preferences. Clicking the link either takes you to a form that asks for personally identifying information, or to a site that downloads malware onto your computer.

Another delivery scam involves fake "missed delivery" tags. Scammers place a note on your door that claims they are having challenges delivering a package to you. They ask you to call a phone number to reschedule your delivery, but it's really a ruse to get your personal information.

Avoid these scams by taking time to verify messages or emails from delivery carriers. Get more info on how to avoid this scam and 10 Steps to Avoid All Scams from the BBB. *Source BBB. org

More Fake Shopping Sites

Reports of fake shopping websites are on the rise. Scammers are much better at creating professional sites and then exploiting buyer protection programs like PayPal to rip-off consumers.

How it Works: You're shopping online and find a site with amazing deals, often brand name goods at a significant discount. The website and the products look legitimate, so you decide to take a chance and make a purchase. The site instructs you to pay through PayPal, which should provide extra security.

After checkout, you get a confirmation email that contains a tracking number from UPS, FedEx, or another shipping service. After a few days, you log onto the site and see that your package has been delivered, but no box ever arrived! The shipping company confirms the package was delivered… but to the wrong address. When you try to contact the ecommerce site you find no contact info. In other cases they are unhelpful or simply don't respond. In some cases consumers who filed claims with PayPal were told that because the crooks provided proof of delivery, the claims weren't paid! Since then PayPal and the major delivery carriers are working to identify these bogus sites and have been more responsive to claims. Avoid these scams by knowing your rights and responsibilities with online payments. Confirm sites have real contact info and try it. If items are selling for much less than elsewhere be on alert. Review online shopping tips.

For more resources on shipping fraud, see FedEx's website and UPS's online resource center. To learn more about scams, go to BBB.org/ScamTips. * Source BBB. org