@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

November 2019

CELEBRATING THE HOLIDAY SEASON ONLINE SAFELY AND SCAM FREE

Our focus this issue is fighting back against scams that are everywhere this time of year. Take advantage of these tips and tools for a safer online holiday season.

— ***Solomon Adote***, **Chief Security Officer**

FAKE SEASONAL JOB SCAMS

The National Retail Federation (NRF) predicts that retailers will hire between 530,000 and 590,000 temporary workers over the 2019 winter holiday season. Many people are eager to find holiday side gigs and many scammers are out there waiting for them.

The Better Business Bureau says to beware of scam job postings, fake recruiter emails, and work-at-home schemes. Always be wary of secret shopper positions, or any generic job title such as caregiver, administrative assistant, or customer service rep.

Unusual hiring procedures should raise suspicion. Watch out for on-the-spot job offers. You may be an excellent candidate for the job, but beware of offers made without an interview. Spammers send out emails promising non-existent jobs for which, upon your application, you'll be asked to pay a commission or fee up front for the job. Similar ads appear in newspaper classifieds and even flyers or signs posted around town. Even if the job exists, you may be conned into working for nothing — with the promise of a generous payment at the end.

Never pay for a job. Even legitimate agencies that earn their money by finding work earn their fees from employers not employees.

GRINCHES TRYING TO STEAL YOUR STUFF

They're here. Scammers can reach right through that small screen in your hand – your smartphone. Consumers are less wary on social media particularly during the busy online shopping season. A new scam report based on BBB Scam TrackerSM data shows that 91% of consumers exposed to a scam on social media engaged with the scammer and 53% of them lost money. Security analysts report that over half of all social media logins are fraudulent, and one-fourth of new account applications are fake.

Grinch-like Phishers are busy gathering information about you and creating convincing fake email accounts to pose as your friend, bank, or a retailer you trust. As criminals gain access to more information about people, Internet fraud attempts become more sophisticated and narrowly targeted. Invitations to see photos of family or friends, email greeting cards and online games/quizzes are all popular during the holiday season. Bogus URLs may link to imitations of legitimate, popular websites, such as eBay, Amazon, or personal banking sites.

PROTECT YOUR DATA AND YOUR WALLET

- **Hover over URLs before you click -** Don't assume that what you see is where you'll go when you click. Hovering over a link, **without** clicking, permits you to see the actual URL for the link. If the underlying link is different, don't click on it. Be extra cautious of links using URL shortening services like tiny URL, Bitly, etc. Got a question about a retail link's validity? Google the intended vendor and go to the site directly.
- **To Friend or Not to Friend -** Scammers take advantage of people looking to connect or reconnect with friends and family this time of year. Be wary of Friend requests from your active online friends. Don't engage with unknown senders on Messenger. Don't assume a friend of an online friend is one.
- **Watch Your Apps** -Your mobile device can be filled with apps running in the background or using default permissions you didn't approve. Say NO to unnecessary privilege requests and ONLY download apps from trusted sources and retailers.

Information provided by the Better Business Bureau

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.