NEWS
CYBER SECURITY
Vol. 5 | Issue 10
November 2020

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

The holiday season is upon us! We are just a few weeks from Thanksgiving Day and a little over a month away from Christmas! And just like everything else this year, it seems, these holidays will be anything but typical. From the way we gather with family (or don't) to how we shop for gifts and hunt down deals, the 2020 holiday season will be unlike any other we've experienced.

One constant, however, will be the scammers who look to take advantage of this opportune time. With Black Friday, Cyber Monday, and holiday shopping come cyber-crimes, frauds, and scams. And, with many retailers releasing their deals earlier and pushing more deals online in response to the ongoing pandemic, the chances for successful scams will dramatically increase.

Last November, Cyber Monday topped the record books with $9.4 billion in sales, and the first year in history that we spent over $3 billion from our smartphones, according to Adobe Analytics. They also reported that between November 1 to December 1, 2019, consumers spent $72.1 billion online. While it is not expected for us to reach those numbers this year, it's definitely worth noting the potential payday for criminals. Fraudsters are well-aware that a vast amount of our Black Friday and Cyber Monday purchases will most likely happen from the comforts of our homes, and they are online and ready.

Here are a few ways to stay safe while shopping for gifts:

- **As always, be suspicious of unsolicited emails.** That is especially true for those with attachments. If you subscribe to a favorite merchant, you should still be careful. Instead of clicking on the email, type the business URL into your browser and look for the deal on their website. If it's not there, you know it was a scam.
- **Use a secure Wi-Fi.** Using public Wi-Fi to shop online while at your favorite coffee shop is tremendously convenient, but it is not cyber safe. Don't make purchases via public Wi-Fi; instead use a Virtual Private Network (VPN) or your phone as a hotspot.
- **Consider your payment options.** Using a credit card is much better than using a debit card; there are more consumer protections for credit cards if something goes awry. Or, you can use a third-party payment service instead of your credit card. There are many services you can use to pay for purchases without giving the merchant your credit card information directly.
- **Keep tabs on your bank and credit card statements.** Be sure to continuously check your accounts for any unauthorized activity. Good recordkeeping goes hand-in-hand with managing your cyber security. Also, set up alerts so that if your credit card is used, you will receive an email or text message with the transaction details.

Cyber Risk Management

This month, we are diving into the practice of "data classification."

Data classification is a way of evaluating data based on its level of sensitivity and the potential impact to DPS if it is shared, altered, or destroyed without authorization, and then assigning a classification to that data. Once data is classified, it can be labeled or marked in such a way to raise awareness and empower the end user (that's you!) to properly handle and protect that data. Data classification is also essential to our Cyber Security team to properly secure and monitor our agency's critical information to help reduce the risk of data leaks or business interruptions that could have a large impact.

DPS data is classified into one of four possible categories:

- **Public** - Information that is collected and maintained by the Department and is subject to public release under the provisions of applicable state or federal law or legal agreement and is not confidential.

- **Sensitive** - Information that is collected and maintained by the Department that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law or legal agreements.

- **Confidential** - Information as defined in Texas Administration Code § 202.1 (5) that is collected and maintained by the Department that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law or other legal agreements.

- **Regulated** - Requires the Department to implement specific privacy and security safeguards as mandated by Federal and State law.

You're probably asking, why do I need to know this? Data classification is actually the responsibility of the Data Owner. In other words, the DPS Division that is responsible for collecting and using the data is also responsible for classifying the data. When it comes to data protection, as the old saying goes, "Knowing is half the battle."

Since we all use data on a daily basis, it is important that we know how to handle that data.

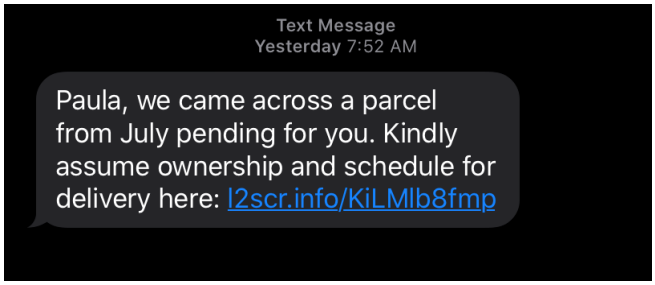
1. What data can and cannot be shared and with whom?
2. What data should be sent via encrypted email vs. normal email vs. not emailed at all?
3. What data should be locked up at night vs. left out on a desk?

These are some examples of questions that you might ask yourself. If you are unsure of the data classification for specific data you'll want to check with your Division leadership. As always, the Cyber Security Risk Management team is here to help with these discussions and can provide guidance in this area (GRP_Cyber_Risk@dps.texas.gov). More information and the complete Data Classification policy can also be found in General Manual chapter 25.04.00 and General Manual chapter 26 Annex.

Text Message Phishing (Smishing)

We have received a few questions regarding phishing attempts via text messages (SMS messages), known as "smishing." As a matter of fact, we've had a few users report malicious links sent to their DPS cell phones. And I, myself, have been receiving a number of these to my personal device.

So what is smishing?



Smishing is a cyberattack that uses misleading text messages to deceive victims. Much like phishing emails, the goal is to trick you into believing that a message has arrived from a trusted person or organization, and then convincing you to take action that gives the attacker exploitable information (like bank account login credentials, for example) or access to your mobile device.

These attacks are successful because although we are all drilled on phishing and scam emails, we are often less watchful for suspicious messages on our phones than on our computers. We're more likely to open a potentially suspicious text message than an email message, and our personal devices generally lack the type of security available on corporate PCs. And, since mobile phones are so widely used, the attack vector is attractive to scammers. In fact, a Gartner study shows 98% of all text messages are read and 45% are responded to, while the equivalent numbers for email are 20% and 6%, respectively. As we grow more overwhelmed by constant emails and suspicious of spam and more and more drawn to mobile phone use, scammers are taking advantage of us and exploiting the more intimate relationships we have with our phones and propensity to interact with text messages.

And, again, as we head into the holiday season and will be shopping more online, we will also be expecting packages on our doorstep. It will be really easy to fall for a smishing attack with a text message stating there was an issue with our last order or a lost package needing to be claimed. Don't fall for the trick!

Ways to stay safe from smishing attacks:

- Be wary of texts using unnatural or ungrammatical language.
- Recognize when a message urges you to take action by clicking a link; then avoid clicking.
- Keep in mind, offers that seem too good to be true usually are.
- Don't click embedded links or download apps directly from a text message.
- Remember, the IRS and Social Security Administration don't communicate via text.
- If you think the message might be real, contact the company using a phone number or website you know is real, not the information in the text message.

In the News

60 Charged in $300M Phone Scam Targeting Elderly Victims

(Associated Press | October 28, 2020)

Sixty people have been charged in a widespread magazine telemarketing scam that authorities say netted $300 million from more than 150,000 elderly and vulnerable people nationwide, the U.S. attorney's office in Minnesota announced Wednesday.

U.S. Attorney Erica MacDonald called the scam the largest elder fraud scheme in the country.

MacDonald said the 60 defendants face a host of charges, including conspiracy, mail fraud, wire fraud, and violating the Senior Citizens Against Marketing Scams Act of 1994. The defendants are from 14 states and two Canadian provinces.

Unfortunately, we live in a world where fraudsters are willing to take advantage of seniors, who are often trusting and polite. It's my hope that this prosecution is a call for vigilance and caution," MacDonald said in a statement.

The indictments and other court documents say that over the last 20 years, the defendants used a network of dozens of fraudulent magazine sales companies and telemarketing call centers to carry out the scam. Employees allegedly used deceptive sales scripts to trick people into making large or repeat payments to the companies.

The indictments allege that many of the defendants used a fraudulent "renewal" script in which the telemarketers falsely claimed to be calling from the victim's existing magazine subscription company with a phony offer to reduce monthly subscription costs.

In reality, the callers had no existing relationship with victims and signed them up for expensive, new magazine subscriptions. As a result, consumers ended up having multiple subscriptions with fraudulent magazine companies.

"Using a tactic like telemarketing magazine sales, these deceitful scam artists bilk hard earned money from their aging victims – leaving so many financially devastated in their retirement years and without recourse for recovery," Michael Paul, the FBI's special agent in charge in Minneapolis, said.

Full Story: https://apnews.com/article/minnesota-minneapolis-3d883c341be205e20b1677f2dba390d5

A Few More Cyber News Stories:

Education Sector Facing Disproportionate Level of Spear-Phishing Attacks
https://www.infosecurity-magazine.com/news/education-disproportionate-spear

European ransomware group strikes US hospital networks, analysts warn
https://www.cyberscoop.com/ransomware-hospitals-ryuk-fireeye/

'Perception Hacks' and Other Potential Threats to the Election
https://www.nytimes.com/2020/10/28/us/politics/2020-election-hacking

CYBER CHALLENGE

See Something?

This Month's Challenge

For this month's challenge, let's see how well you pay attention to your surroundings!

The national "If You See Something, Say Something™" campaign was developed to raise public awareness of indicators of terrorism and terrorism-related crime, and to emphasize the importance of reporting suspicious activity to the proper authorities. Cyber security awareness has adopted this mentality as a way to report suspicious online activity and help thwart cyber crime.

That same "see something, say something" concept is a great way to help us protect DPS. If something seems weird about an email or someone seems out of place, say something. Be vigilant. For example, if you receive an email that just doesn't seem legit, forward the email as an attachment to SPAM@dps.texas.gov or contact the Service Desk. For other scenarios that raise a cyber security alarm, contact GRP_Cyber_Security@dps.texas.gov.

Of course, the same applies to physical security. If someone is loitering by a locked door or digging through a dumpster, say something.

But, before you're able to say something...you must be able to spot something out of the ordinary, right?

Here's the challenge — head on over to this website provided by DHS and to find out how well you pay attention to your surroundings. https://www.dhs.gov/see-something-say-something/take-challenge