NEWS
CYBER SECURITY
Vol. 7 | Issue 11 November 2022

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

We hope this newsletter finds you and your families doing well as we head into the holiday season!

1 big thing: Now that the student loan debt relief application is open, spot the scams.

What to know: The Department of Education (ED)'s application for federal student loan debt relief is now open and, of course, scammers are on the move — trying to get your money and personal information.

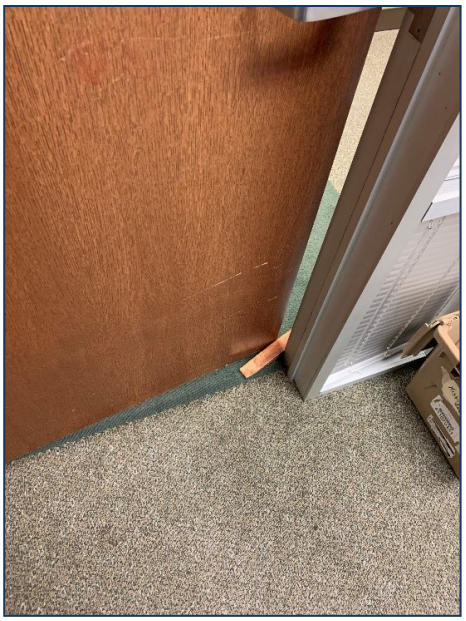
How to protect yourself: The Federal Trade Commission (FTC) has offered some advice to steer clear of scammers.

- To apply, navigate to "StudentAid.gov/DebtRelief". Nowhere else. Be wary of links that look like this one in phishing emails. Best practice is to type the URL in a browser instead of clicking a link.
- **Don't pay to apply.** It's FREE. Anyone who says you need to pay is a scammer.
- **Know what to share, where, and when.** The real application will ask for your name, birth date, Social Security number, phone number, and address. You don't have to upload or attach any documents.
- **Know what not to share.** When you apply, nobody legit will ask for your FSA ID, bank account, or credit card information.
- ·**Expect email updates from ED.** After you apply, you may hear from ED to give updates on your application or ask for documents.
    - Those emails will only come from noreply@studentaid.gov, noreply@debtrelief.studentaid.gov, or ed.gov@public.govdelivery.com.
    - Pay close attention the sender address for emails about loan forgiveness — looking for slight typos — to avoid a scammer's fake emails.
- **Follow ED's process if your application is denied.** Anyone who says they can get you approved (for a fee) is a scammer

For more information: https://consumer.ftc.gov/consumer-alerts/2022/10/now-student-loan-debt-relief-application-open-spot-scams

Physical Security Matters Too

Physical security is an important aspect of cyber awareness. It includes the protection of people, property, and physical assets from actions and events that could cause damage or loss.



Here are a few tips and best practices:

- **Do not prop open doors.** This is usually seen in areas where the doors are supposed to be locked and secured. However, this practice is used for pure convenience. Propped-open doors causes risk to the property as well as all people inside the facility.
- **Lending your access card out to someone else is not a good idea.** Your badge has access related to your job functions and keeps record of all badge swipes when used. If an investigation is opened for whatever reason, and your badge is used to swipe into an area in question, you will be questioned.
- **Do not allow tailgating.** Allowing people to enter on your badge swipe is a breach of security. So is following people into a secure area without using your access card. Allowing unauthorized people into buildings could cause you to be investigated and puts people and property at risk.
- **Stay alert and vigilant while walking too and from parking lots**, garages, and buildings. Your personal awareness can save your life. If you are preoccupied and are not aware, your reaction to threats is lowered and your risk of harm is greater.
- **Know your evacuation routes** whether in buildings, lots, garages, or surrounding areas. Having a plan of action for the "just in case" situations keeps you a few steps ahead of the threat or act of violence.
- **When you have visitors and or deliveries,** make sure that proper procedures are followed when allowing these people into secure facilities. There may be a policy in place that requires all visitors to sign in and be always escorted. Secure facilities may have a certain procedure to follow to receive and pickup deliveries.

In the News

DHL Replaces LinkedIn As Most Imitated Brand in Phishing Attempts

(Alessandro Mascellino | October 24, 2022)

Shipping company DHL has knocked LinkedIn off the top spot as the number one brand being imitated in phishing attempts between July and September.

The data comes from Check Point's Q3 *Brand Phishing Report*, which the company shared with *Infosecurity* earlier today.

According to the new data, DHL now accounts for just under a quarter (22%) of all phishing attempts worldwide. Check Point has said this is due partly to a significant global scam and phishing attack that the logistics firm warned about days before the quarter started.

Microsoft is in second place (16%), and LinkedIn has fallen into third, accounting for just 11% of scams, compared to 52% in Q1 and 45% in Q2.

"In Q3, we saw a dramatic reduction in the number of phishing attempts related to LinkedIn, which reminds us that cyber-criminals will often switch their tactics to increase their chances of success," said Omer Dembinsky, data research group manager at Check Point.

"It is still the third most commonly impersonated brand, though, so we'd urge all users to stay mindful of any emails or communications purporting to be from LinkedIn."

As for industries most affected by phishing in Q3, shipping resulted at the top in the Check Point report, followed by technology.

"Now that DHL is the brand most likely to be imitated, it's crucial that anyone expecting a delivery goes straight to the official website to check progress and/or notifications," Dembinsky warned. "Do not trust any emails, particularly those asking for information to be shared."

Full Story: https://www.infosecurity-magazine.com/news/dhl-top-spot-most-imitated-in/

A Few More Cyber News Stories:

Spy agency embraces meme culture and the internet is here for it
https://www.cyberscoop.com/nsa-memes-cybersecurity-awareness/

Samsung Galaxy Store Bug Could've Let Hackers Secretly Install Apps on Targeted Devices
https://thehackernews.com/2022/10/samsung-galaxy-store-bug-couldve-let.html

Experian tool exposed partial Social Security numbers, putting customers at risk
https://www.cyberscoop.com/experian-kbv-ssn-nist-identity-theft/

CYBER CHALLENGE

Breach

This Month's Challenge

For this month's challenge, let's kick it old school and play a computer game using the arrow keys on your keyboard! Remember those days?

In this game, you'll roam around the gaming map looking for laptops and identifying what went wrong during a massive data breach.

Let me know how many laptops you find! (Hint: there are 16 total)

Good luck! (avg. play time: 15min)

https://www.educationarcade.co.nz/breach