NEWS
CYBER SECURITY
Vol. 7 | Issue 6
June 2022

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

We still have a few weeks until it's officially summer, but hopefully those summertime vibes and vacations are already cranking up for you. Congrats to all with graduates this year!

1 big thing: Cryptocurrency is crashing; don't fall for "easy digital money" scams

bitcoin
GIVEAWAY
ethereum
giveaway
visit one of the websites:

What to know: Cryptocurrency has always been volatile, but now its downward slide has generated plenty of headlines. And, as with anything that is newsworthy, scammers are taking advantage of the media coverage.

The latest threat: Recent YouTube videos (some allegedly shared "live") have seemed to feature famous technology entrepreneurs endorsing a supposed cryptocurrency giveaway, or opportunities to double cryptocurrency investments. However, these videos were simply edited together using existing footage of the individuals featured. Scammers directed victims to malicious websites designed to resemble legitimate cryptocurrency and financial exchanges where they stole credentials and drained victims' accounts.

Keep these tips about crypto scams in mind while online:

- Be suspicious of cryptocurrency opportunities that seem too good to be true. Remember: even the most successful investors can't guarantee a profit.
- Verify the legitimacy of any cryptocurrency opportunity before you invest.
- A familiar face, name, company, or social media account can't always be trusted. Celebrity endorsements and testimonials can be easily faked.

Not sure what Cryptocurrency is? You're not alone.

Learn more here: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

Why Cyber Awareness Training?

Why do we even need cyber awareness training? Great question!

A few weeks ago, a DPS Deputy Director testified before the Texas Senate Committee on Business and Commerce about cybersecurity and stressed the importance of cyber awareness.

As part of his testimony, he stated, “No amount of spam filters, antivirus software, end point detection and response tools, or detailed assessments on controls can replace the value of workforce that, on a daily basis, adopts complete responsibility for their network security.

In a recent study conducted by IBM, it was discovered that human error was a major contributing cause in 95% of all breaches. Mitigation of human error must be a key component to cyber business security as we move forward.

This starts with cyber security awareness training. That should be followed by additional cyber security awareness training, and once that’s complete, employees should undergo further cyber security awareness training.”

He continued, “The benefit of the cyber security awareness program is not that it will make everyone who undergoes the training program a cyber security expert but more importantly provides a heightened awareness of the issue.

It has to become important to everyone.”

And, naturally, we couldn’t agree more!

As a reminder, attackers today rarely attack businesses through technology means only. Today’s attackers target people as an “easier way” into protected networks. They take advantage of our curiosity, propensity to react to urgency, and natural willingness to help somebody in need. And they succeed when they can capitalize on lack of awareness. It’s much easier to trick a human (or take advantage of a mistake) than to hack a system, generally.

When employees are cyber aware:

- We all understand what cyber threats are and the potential impact they’ll have on our organization.
- We know the steps to take to reduce and prevent cyber-crime from infiltration our workspace.
- We can better-protect our resources and sensitive data in our homes.
- We are empowered as a united front to protect and serve our customers.

In the News

Texas man gets 5 years for stealing 38,000 PayPal account credentials

(Suzanne Smalley | May 12, 2022)

A Texas man whom federal prosecutors say bought 38,000 compromised PayPal account credentials from an illegal online marketplace and used them to steal from the true account owners was sentenced to five years in prison Wednesday, the Justice Department said.

Marcos Ponce, 37, of Austin, also was ordered to pay $1.4 million in restitution, according to a Justice Department press release, which said Ponce pleaded guilty to conspiracy to commit wire fraud in October 2021.

Court documents in the case show that from at least November 2015 until November 2018, Ponce and his co-conspirators established buyer accounts on an illegal online marketplace which sold stolen payment account credentials along with complementary personal identification information.

Prosecutors contend that Ponce and his co-conspirators developed social engineering techniques so they could dupe third parties into accepting money transfers from the compromised PayPal accounts before transferring the money into accounts they controlled.

"The Justice Department remains firmly committed to protecting the American people from fraudsters like this defendant," Assistant Attorney General Kenneth Polite, Jr. of the Justice Department's Criminal Division said in a prepared statement. "May today's sentencing send a clear message to would-be thieves: there are real-world consequences for online crimes."

PayPal account credentials have proven a popular lure for cybercriminals. In August fraudsters impersonating the head of Europol, the European Union's law enforcement agency, threatened targeted individuals with criminal prosecution before attempting to steal their PayPal account credentials.

Full Story: https://www.cyberscoop.com/marcos-ponce-paypal-credentials-prison/

A Few More Cyber News Stories:

iPhones Vulnerable to Attack Even When Turned Off
https://threatpost.com/iphones-attack-turned-off/179641/

Cyber security: Global food supply chain at risk from malicious hackers
https://www.bbc.com/news/science-environment-61336659

Elon Musk deep fakes promote new BitVex cryptocurrency scam
https://www.bleepingcomputer.com/news/security/elon-musk-deep-fakes-promote-new-bitvex-cryptocurrency-scam/

CYBER CHALLENGE

Find the Phish

This Month's Challenge

For this month's challenge, let's get back to practicing spotting phishing emails vs legitimate ones.

There are 4 emails to look over and decide whether they are phishy or real. The answers are on the same page…so try not to peek!

Let me know how you do, and ask any questions that may come up. You got this!

https://ermprotect.com/blog/paypal-netflix-uber-phishing-attempts/

Once you're done with those, head over to their blog page and check out the rest of the "Spot the Phish" posts. Admittedly, the blog hasn't been updated in a bit, but the content is still applicable and worth checking out!

The more you train, the easier phishing emails are to spot!

https://ermprotect.com/spot-the-phish/