NEWS
CYBER SECURITY
Vol. 7 | Issue 9
September 2022

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

It's fall, y'all! Well, not officially, but school is back in session, football is back on TV, and pumpkin spice is all over H-E-B...so...it's pretty much here! Hope this newsletter finds you healthy and ready for cooler weather.

A major corporation was breached a few weeks ago. An employee misused their company credentials with poor cyber hygiene involving a personal Google account. Their personal account was hacked which opened the door to their company credentials...and, in turn, access to the corporate network.

From our Cyber Security Cloud Security Architect:

It's important for company employees to continue to remain alert for any suspicious activity regarding their credentials.

Recently, the infrastructure of a private sector partner was compromised, and it all began with an employee's personal Google account being hacked. The employee had opted to store their company username and password within Google Chrome for convenient recall when logging into company resources within Google Chrome.

By default, this action synchronizes the credentials to a user's Google account if they are logged into Chrome with their personal Google account. By targeting this employee's insecure personal Google account, the attacker was able to retrieve the employee's company credentials.

The attacker then used these credentials to try and log into the company's VPN and caused a flood of multi-factor requests to the employee to approve access (think text messages, or push notifications to approve access). The employee approved one of those requests thinking this would 'stop the flood'.

This seemingly minor action granted the attacker access to the company's infrastructure, and the attacker was then able to scout the network and exfiltrate data.

Here are a few key reminders that we can all learn from this event:

- Never store credentials within a browser on your workstation or your phone (or write them down for that matter).
- If you get a flood of requests to your mobile device, turn off your phone and contact your HelpDesk immediately.

In the News

Why Robotexts are Scammers' Favorite New Tool

(Tonya Riley | August 10, 2022)

If you've recently received a text claiming to have a delivery update for a package you never ordered or providing an urgent security alert for a bank you don't belong to, you're not alone.

So far in 2022, the Federal Communications Commission has received more than 8,500 complaints about "unwanted text messages," according to a consumer alert released last month.

That number is on track to surpass the number of complaints in 2021, which included 15,300 messages. But according to industry data, the number is likely just a small sliver of the problem. Spam-blocking app RoboKiller estimated that consumers received more than 12 billion robotexts in June alone.

Like robocalls, robotexts aren't just a nuisance — they're a powerful tool for scammers. In fact, experts say that in some ways scam text messages can be even more dangerous than robocalls. With one click, a victim could be tricked into providing information used to hack into their bank account or work email.

"I would argue that, in a way, robotexts are actually more dangerous," said Teresa Murray at Public Interest Research Group, a consumer watchdog group. "Maybe not more annoying, but more dangerous because it's more difficult for consumers to determine whether a robotext is legitimate or not."

Part of the increase in texts, Murray says, stems from a decrease in robocalls. Since an FCC mandate requiring all voice providers to implement call verification software went into effect last summer, robocalls declined by nearly 50 percent, according to a report from her group. More than half of U.S. phone providers have since implemented some sort of robocall mitigation software for voice calls, forcing scammers into a new line of business.

Full Story: https://www.cyberscoop.com/robotext-scam-fcc-malware-smishing-phishing/

A Few More Cyber News Stories:

Nelnet Servicing breach exposes data of 2.5M student loan accounts
https://www.bleepingcomputer.com/news/security/nelnet-servicing-breach-exposes-data-of-25m-student-loan-accounts/

Google researchers expose Iranian hackers' tool to steal emails from Gmail, Yahoo and Outlook
https://www.cyberscoop.com/google-iran-hackers-gmail-irgc-charming-kitten/

Nitrokod Crypto Miner Infected Over 111,000 Users with Copies of Popular Software
https://thehackernews.com/2022/08/nitrokod-crypto-miner-infected-over.html

CYBER CHALLENGE

Protect & Connect

This Month's Challenge

For this month's challenge, let's do something a little different.

Let's train to be Internet Bodyguards!

The National Cybersecurity Alliance teamed up with Amazon to create a few short videos (that are really well-done, in my opinion) to help you fend off cybercriminals. Recognize a few of the actors?

Once you're trained up in their dojo, take the quiz and let me know how you do. It might actually be a little too easy for you; let me know if that's the case!

Also, for bonus points, let me know how many friends and family members you share this with! Have fun!

https://protectconnect.com/en/index.html