NEWS
CYBER SECURITY
Vol. 9 | Issue 7
July 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Summer Is in Full Swing…And So Are The Summertime Scams

What to know: As the summer season heats up, scammers know we are a little more relaxed and a little less diligent with our cyber awareness as we are distracted with vacations and pool parties. Here are a few things to look out for this summer, even as you take that well-deserved break.

Summer Travel Security

- Public Wi-Fi: avoid connecting to public Wi-Fi; if you have to use it at an airport or hotel, use a VPN.

Summer Sale Scams

- Fake deals: verify the authenticity of websites offering summer deals and discounts.
- Secure payments: look for "https" in the website URL when shopping online.

Social Media Precautions

- Vacation announcements: posting real-time updates about your plans can be exploited.
- Geotagged photos: disable geotagging, if possible, to avoid sharing your exact location.

Seasonal Phishing Attacks

- Weather-related scams: be wary of emails about hurricanes, heatwaves and other emergencies. Scammers love to exploit these events by including malicious links and attachments to emails.

Summer Event Scams

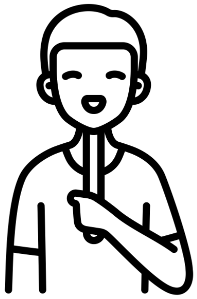
- Event tickets: always buy tickets from official and reputable sources when attending summer concerts, festivals, and other events.

Other summer cyber tips: https://staysafeonline.org/resources/vacation-and-travel-security-tips

Social Engineering

Social engineering is when cybercriminals trick you into giving up your personal information.

Instead of hacking into systems directly, they manipulate you into revealing confidential info like passwords or financial details. Think of it as a high-tech con game where deception is the main tool. Why spend time and resources hacking into a system when they can just ask you for your password?



Created by Victoruler from Noun Project

The most common types of social engineering:

- **Phishing**: This involves sending fake emails that look like they're from a trusted source, like your bank or a popular website. The goal is to get you to click on a link or provide sensitive info.
- **Pretexting**: In this scam, the attacker creates a made-up story to steal your information. For instance, they might pretend to be a co-worker or an authority figure to get details from you.
- **Baiting**: This trick involves offering something tempting, like a free music download or a USB drive labeled with interesting content left in a public place, to lure you into the scam.
- **Tailgating**: Also known as "piggybacking," this is a physical tactic where someone follows an authorized person into a restricted area without permission.

Tips to recognize and avoid social engineering:

- **Be skeptical of unexpected requests.** If you get an email or call out of the blue asking for personal info, that's a red flag. Verify the person's identity through official channels before sharing any details.
- **Look for other red flags.** Phishing emails often have urgent language, spelling mistakes, or generic greetings. Trust your instincts - if something feels off, it probably is.
- **Double-check links before clicking.** Carefully hover over links to see the actual URL. If it looks suspicious or doesn't match the supposed source, don't click.
- **Use multi-factor authentication (MFA):** This adds an extra layer of security by requiring at least two forms of verification before you can access your accounts.
- **Stay informed.** Keep yourself updated on the latest social engineering tricks and share this info with friends, family, and colleagues.

Go deeper: https://blog.knowbe4.com/five-signs-of-social-engineering

In the News

Microsoft informs customers that Russian hackers spied on emails

(Zeba Siddiqui | June 27, 2024)

Russian hackers who broke into Microsoft's systems and spied on staff inboxes earlier this year also stole emails from its customers, the tech giant said on Thursday, around six months after it first disclosed the intrusion.

The disclosure underscores the breadth of the breach as Microsoft faces increasing regulatory scrutiny over the security of its software and systems against foreign threats. An allegedly Chinese hacking group that separately breached Microsoft last year stole thousands of U.S. government emails.

The Russian government has never responded to the Microsoft hacking allegations, but Microsoft has said the hackers targeted cybersecurity researchers who had been investigating the Russian hacking group's actions.

"This week we are continuing notifications to customers who corresponded with Microsoft corporate email accounts that were exfiltrated by the Midnight Blizzard threat actor," a Microsoft spokesperson said in an emailed statement. Bloomberg first reported on the action earlier in the day.

Microsoft said it was also sharing the compromised emails with its customers, but did not say how many customers had been impacted, nor how many emails may have been stolen.

"This is increased detail for customers who have already been notified and also includes new notifications," the spokesperson said. "We're committed to sharing information with our customers as our investigation continues."

Full Story: https://www.reuters.com/technology/cybersecurity/microsoft-tells-clients-russian-hackers-viewed-emails-bloomberg-news-reports-2024-06-27

A Few More Cyber News Stories:

Apple Patches AirPods Bluetooth Vulnerability That Could Allow Eavesdropping
https://thehackernews.com/2024/06/apple-patches-airpods-bluetooth.html

Explained: Android overlays and how they are used to trick people
https://www.malwarebytes.com/blog/news/2024/06/explained-android-overlays-and-how-they-are-used-to-trick-people

The Secrets of Hidden AI Training on Your Data
https://thehackernews.com/2024/06/the-secrets-of-hidden-ai-training-on.html

CYBER
CHALLENGE

Spot the Phish Practice

This Month's Challenge

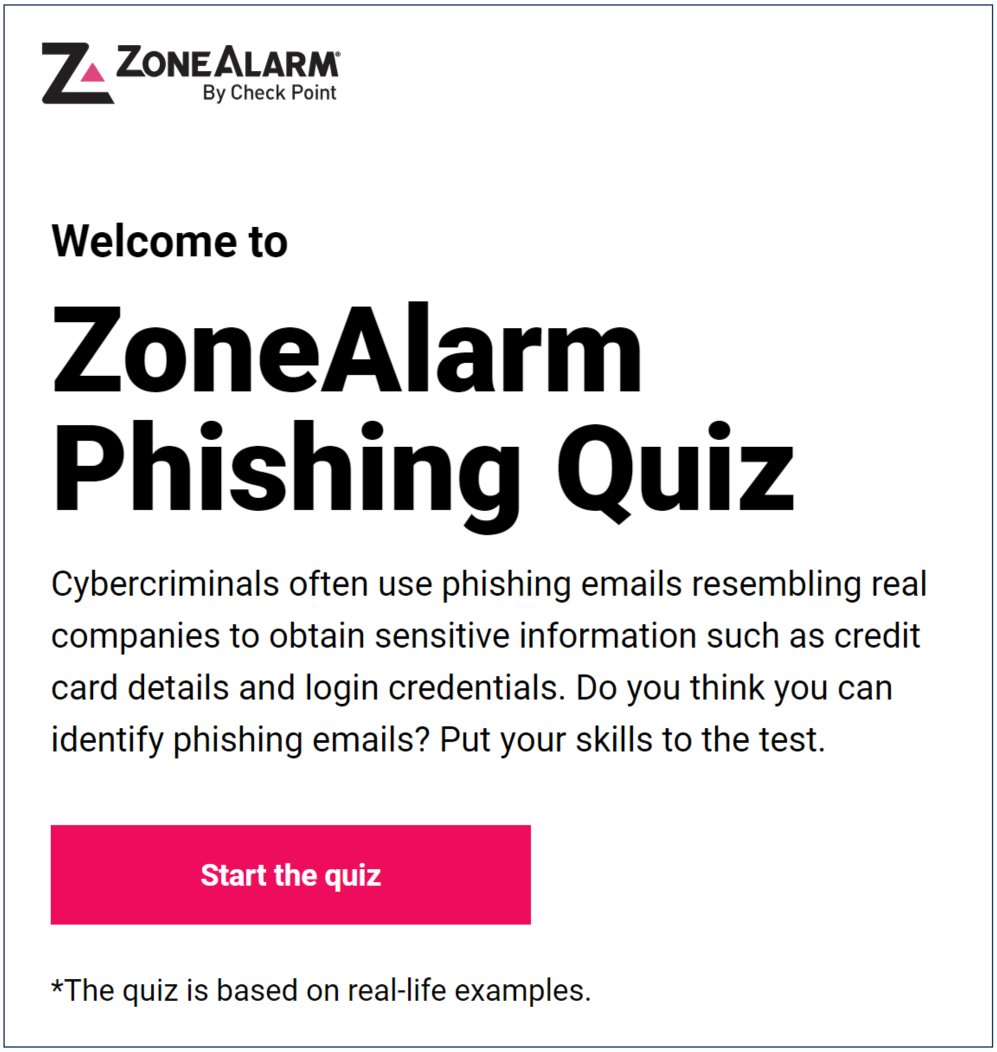
For this month's challenge, let's practice spotting the phish!

You'll have 10 emails to look at and decide whether they are phishing or genuine.

Make to sure to look carefully; some of these are tricky!

Let me know how you do. Good luck!

https://www.zonealarm.com/promotions/zonealarm-phishing-quiz



Welcome to

ZoneAlarm Phishing Quiz

Cybercriminals often use phishing emails resembling real companies to obtain sensitive information such as credit card details and login credentials. Do you think you can identify phishing emails? Put your skills to the test.

*The quiz is based on real-life examples.