CYBER SECURITY NEWS
Vol. 7 | Issue 1
January 2022

| Page 2| Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

Happy New Year! May 2022 bring you genuine joy through all the highs and the lows life will undoubtedly bring.

Last year, we opened the 2021 newsletter by sharing news of a big breach involving Solar Winds. This year, there's an even bigger breach circulating the news. This one runs deep and will most likely take years for the global industry to fully patch against it.

You may have heard about the Log4j vulnerability by now; it's been about a month since it was publicly announced. The reason it's such a big deal is because the vulnerable tool is used by organizations and government agencies all over the globe, impacting millions of machines.

In fact, it's been characterized as the single biggest, most critical vulnerability of the last decade, and possibly the biggest in the history of modern computing. One of the reports found online claims more than 840,000 attacks were initiated within 72 hours of vulnerability disclosure and attacks reached over 100 per minute over that first weekend.

If this Log4j vulnerability is exploited by one of these attacks, attackers can weaponize it to do things like steal information or install malware or take complete control of the machine and access the entire network of the breached company.

What is Cyber doing to protect our DPS systems?
DPS Cyber Security continues to diligently scan our network systems for this vulnerability and reach out to System Owners where updates are needed. We've also provided our DPS Contract Monitors and System/Application Administrators for vendor-managed applications with questions to ask vendors and steps to take according to their answers.

What should I do as a DPS staff member?
All users should continue to remain vigilant and report any suspicious activity to Cyber Security.

What can I do to protect myself at home?
The pressure is largely on companies and agencies to act and address the vulnerability. For now, you should make sure to update devices, software, and apps when companies give prompts as they remediate their systems. And, be mindful of phishing messages and scams looking to exploit this widespread panic.

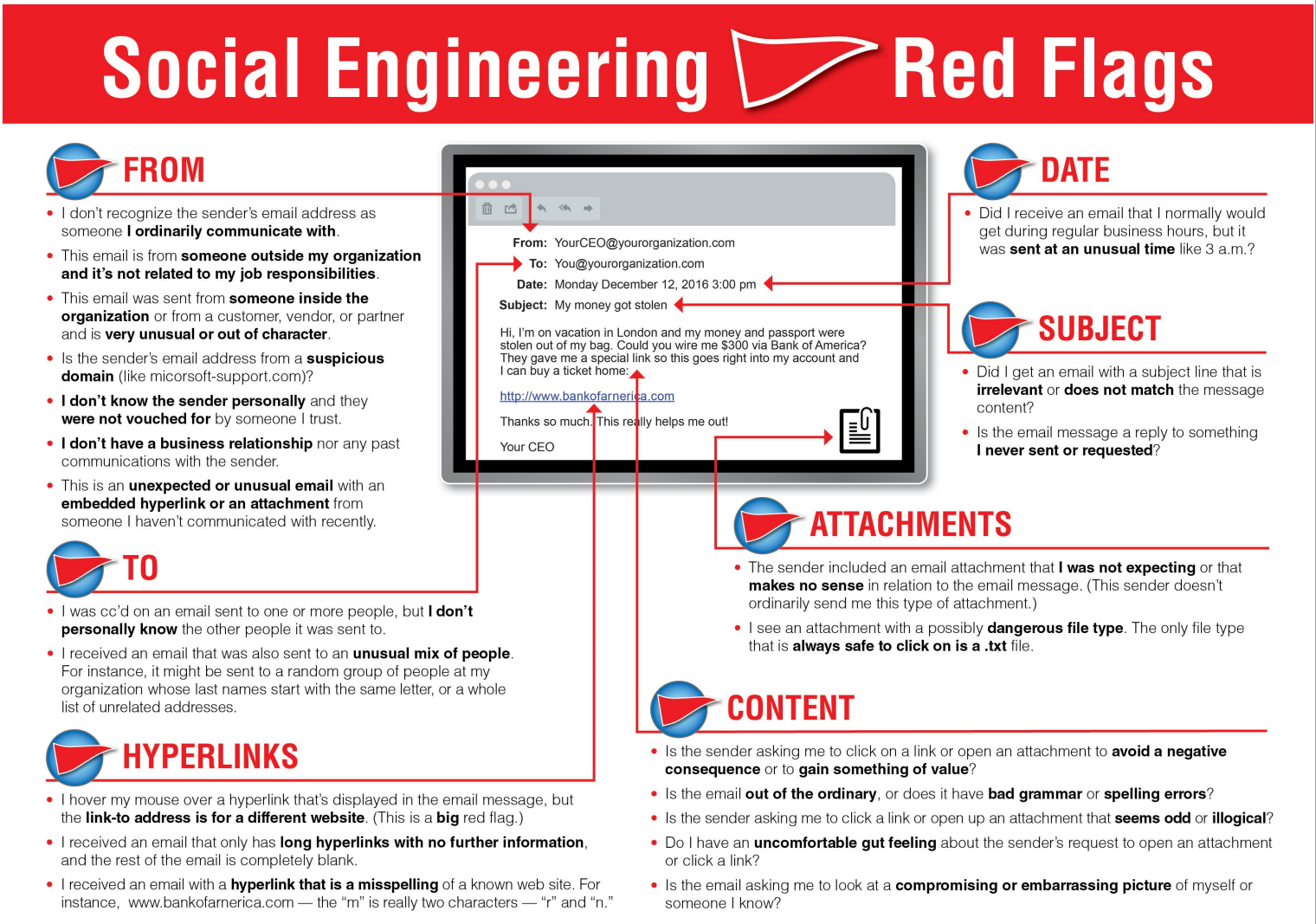
Social Engineering Red Flags

The easiest way to avoid falling for scams and other social engineering attacks is to have a solid understanding of the tactics employed by attackers. Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system.

One of the most common signs of a scam is the use of "stressor events," which play on our emotions to make us act irrationally. There are a wide variety of stressor events, ranging from the mild to the extreme. Scammers can simply try to rush you by claiming that the deal will be called off if you don't act soon, or they can threaten you with arrest or worse if you don't pay them quickly. They can also be used as excuses on the scammer's side, such as a sudden family tragedy affecting their ability to send or receive a transaction. The most popular way to elicit these emotions from us is through phishing emails.

This has been one of my favorite graphics on social engineering red flags for a long time. It does a great job of breaking down red flags typically found in different sections in a phishing email. Please take a few minutes to review this.

(If the text seems a bit too small to read, please use the zoom feature to enlarge it.)

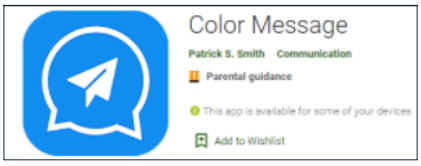


In the News

Malicious Joker App Scores Half-Million Downloads on Google Play

(Tara Seals | December 17, 2021)

Joker malware was found lurking in the Color Message app, ready to fleece unsuspecting users with premium SMS charges.



The Joker malware is back again on Google Play, this time spotted in a mobile application called Color Message. The app was downloaded more than 500,000 times before its removal from the store.

Users should immediately delete Color Message from their devices to avoid being defrauded, researchers at Pradeo Security warned.

Joker is a persistent threat that's been kicking around since 2017, hiding itself within legitimate-seeming, common application types like games, messengers, photo editors, translators and wallpapers, many of them aimed at children. But once installed, Joker apps subscribe victims to unwanted, paid premium services controlled by the attackers – a type of billing fraud that researchers categorize as "fleeceware." Often, the victim is none the wiser until the mobile bill arrives.

In the worst cases, the apps also exfiltrate contact lists and device information and can hide their icons from the home screen – which is the case with Color Message, Pradeo researchers said, adding that the application appeared to be making connections to Russian servers.

Color Message purported to offer the ability to jazz up messaging with a range of fun emojis and screen overlays.

It makes texting easy, fun and beautiful," according to its Google Play listing, captured by Pradeo before the takedown. "Customize the theme quickly. The Color Message application has unique technology that can help you personalize your default SMS messenger."

Interestingly, it also had 1,800+ reviews, with an average rating of four stars – though the more recent reviews tended towards the scathing, such as "misleading ad and worst app ever."

Full Story: https://threatpost.com/malicious-joker-app-downloads-google-play/177139/

A Few More Cyber News Stories:

New Mobile Network Vulnerabilities Affect All Cellular Generations Since 2G
https://thehackernews.com/2021/12/new-mobile-network-vulnerabilities.html

Russian national accused of hacking, illegal trading is extradited to US
https://www.cyberscoop.com/russian-hackers-insider-trading-yermakov-mueller/

CISA Issues Emergency Directive on Log4j
https://www.darkreading.com/threat-intelligence/cisa-issues-emergency-directive-on-log4j

CYBER CHALLENGE

Spot the Red Flag

This Month's Challenge

For this month's challenge, let's practice spotting the red flags found in phishing emails like the ones mentioned earlier in the newsletter.

From our friends over at Living Security, this challenge provides 6 emails to look over. You are to identify the reddest flag within the email. Or you can decide it's legitimate and click the "Legitimate" button.

Let me know how you do, and send me the passcode you receive at the end of the exercise so I know you endured until the end. Good luck! (takes about 10 min. to complete)

Access the challenge here: https://flags.livingsecurity.com/