Vol. 9 | Issue 3

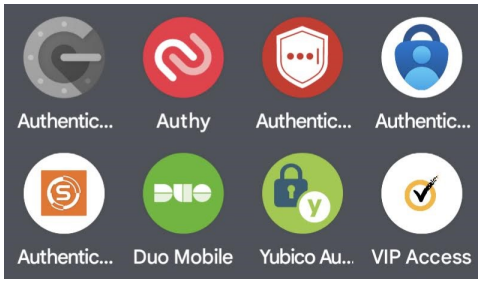
CYBER SECURITY NEWS

March 2024

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: What is an authenticator app, anyway?



What to know: An authenticator app is a tool designed to add an extra layer of security to your online accounts, typically used for services like email, social media, and banking.

Instead of relying solely on passwords, which can be vulnerable to hacking, authenticator apps generate unique codes that you use alongside your password for logging in. This is an example of Multi-Factor Authentication (MFA) – something you know (password) + something you have (the code from the authenticator app on your smartphone). A stat from Microsoft revealed that MFA can block over 99.9 percent of account compromise attacks.

Think of an ATM. They've used MFA for decades. You are required to insert your bank card (something you have) and enter a PIN (something you know); this is MFA to prove you are who you say you are.

How they work: After downloading an authenticator app, you link it to your online account by scanning a QR code or entering a setup key provided by the service.

Once set up, the authenticator app starts generating six-digit codes at regular intervals, usually every 30 seconds.

When you try to log in to your account, along with your password, you're prompted to enter the current six-digit code generated by the authenticator app. (SecureAuth will present a single letter or number matched with the code).

The service verifies the code entered against the one it expects. If they match, you're granted access to your account.

Since the generated codes change every few seconds, it's much harder for hackers to gain unauthorized access to your accounts.

Go deeper: https://www.keepersecurity.com/blog/2023/07/20/what-are-authenticator-apps-and-how-do-they-work

Be Malware Aware

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. Malware can infect your device through various means, such as malicious email attachments, compromised websites, or software downloads.

Once malware infiltrates a device, it can perform a variety of harmful actions, including:

- **Data Theft.** Malware can steal sensitive information such as passwords, credit card numbers, and personal files.
- **System Damage.** Some types of malware are designed to corrupt or delete files, causing system instability or even rendering the device unusable.
- **Remote Control:** Certain malware, such as remote access Trojans (RATs), can give hackers remote control over infected devices, allowing them to spy on users or carry out further attacks.

Ransomware is particular dangerous. It's a specific type of malware that encrypts files on a victim's device and demands payment (a ransom) in exchange for the decryption key. It typically spreads through malicious email attachments, infected websites, or exploit kits. And it can spread through an entire network, locking files of an entire organization. Without the decryption key, the victim may lose access to their files permanently.

To protect yourself against malware and ransomware, follow these tips:

- **Use Antivirus Software.** Install reputable antivirus software and keep it updated to detect and remove malware.
- **Be Cautious Online.** Avoid clicking on suspicious links or downloading files from unknown sources.
- **Backup Your Data.** Regularly backup your important files to an external hard drive or cloud storage service to mitigate the impact of a ransomware attack.
- **Keep Software Updated.** Keep your operating system and software applications updated with the latest security patches to patch vulnerabilities that malware may exploit.

Learn more about various types of malware: https://www.techtarget.com/searchsecurity/definition/malware

Learn more about ransomware and how to prevent it: https://www.cisa.gov/stopransomware

In the News

Your smart TV is tracking you – here's how to disable it

(Mohamed Al Elew | February 2024)

Your smart TV knows what you're watching.

If you bought a new smart TV during any of the holiday sales, there's likely to be an uninvited guest watching along with you. The most popular smart TVs sold today use automatic content recognition (ACR), a kind of ad surveillance technology that collects data on everything you view and sends it to a proprietary database to identify what you're watching and serve you highly targeted ads. The software is largely hidden from view, and it's complicated to opt out. Many consumers aren't aware of ACR, let alone that it's active on their shiny new TVs. If that's you, and you'd like to turn it off, The Markup is going to show you how.

First, a quick primer on the tech: ACR identifies what's displayed on your television, including content served through a cable TV box, streaming service, or game console, by continuously grabbing screenshots and comparing them to a massive database of media and advertisements. Think of it as a Shazam-like service constantly running in the background while your TV is on.

These TVs can capture and identify 7,200 images per hour, or approximately two every second. The data is then used for content recommendations and ad targeting, which is a huge business; advertisers spent an estimated $18.6 billion on smart TV ads in 2022, according to market research firm eMarketer.

For anyone who'd rather not have ACR looking over their shoulder while they watch, we've put together a guide to turning it off on three of the most popular smart TV software platforms in use last year. Depending on the platform, turning off ACR took us between 10 and 37 clicks.

Full Story: https://www.msn.com/en-us/money/other/your-smart-tv-is-tracking-you-here-s-how-to-disable-it

A Few More Cyber News Stories:

Humanoid robots draw millions from Bezos, OpenAI and more
https://www.axios.com/2024/02/29/ai-robot-figure-nvidia-openai-jeff-bezos

Airbnb scammers pose as hosts, redirect users to fake Tripadvisor site
https://www.helpnetsecurity.com/2024/02/29/airbnb-scam

Each Facebook User is Monitored by Thousands of Companies
https://themarkup.org/privacy/2024/01/17/each-facebook-user-is-monitored-by-thousands-of-companies-study-indicates

CYBER CHALLENGE

DOD Cyber Challenge

This Month's Challenge

For this month's challenge, let's see how you do with the U.S. Department of Defense's Cyber Challenge!

Keep in mind, this is geared toward federal employees, but most of the content is applicable since it covers cyber awareness best practices. There may be terms you don't recognize, but that just adds to the fun!

You can choose between the Standard Challenge (ignore the "must select this option" verbiage meant for federal employees) or the Knowledge Check Option. The Standard Challenge will allow you to check out all the activities to earn badges. The Knowledge Check Option will allow you to take a shortcut to the badges based on how you do on the quiz.

Send me a screenshot of the "Challenge Complete" screen...if you get there. If you throw in the towel, send me a screenshot of all the badges you earned along the way.

Good luck!

https://dl.dod.cyber.mil/wp-content/uploads/trn/online/disa-cac-2024/launch.html