CYBER SECURITY NEWS
Vol. 7 | Issue 4
April 2022

| Page 2 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

A protected home network means your family can use the internet more safely and securely.

Most households now run networks of devices linked to the internet, including computers, gaming systems, TVs, tablets, smartphones and wearable devices that access wireless networks.

The first step to protect your home is to keep a clean machine and make sure all of your internet-enabled devices have the latest operating system, web browsers and security software. This includes mobile devices that access your wireless network.

Secure Your Wireless Router

Using Wi-Fi is a convenient way to allow multiple devices to connect to the internet from different areas of your home. However, unless you secure your Wi-Fi router, you're vulnerable to people accessing information on your computer, using your internet service for free and potentially using your network to commit cybercrimes.

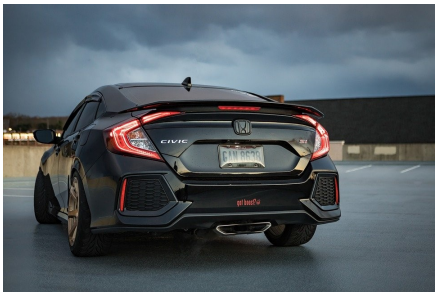
To secure your wireless router:

- **Change the name of your router:** The default ID - called a "service set identifier" (SSID) - is assigned by the manufacturer. Change your router to a name that is unique to you and won't be easily guessed by others.
- **Change the preset password on your router:** Leaving a default password unchanged makes it much easier for hackers to access your network. You should change it as soon as possible.
- **Review security options:** When choosing your router's level of security, opt for WPA2, if available, or WPA – these levels are more secure than the WEP option.
- **Create a Guest password:** Some routers allow for guests to use networks via separate guest passwords. If you have many visitors to your home, it's a good idea to set up a guest network.
- **Use a firewall:** Firewalls help keep hackers from using your device to send out your personal information without your permission. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

More ways to protect yourself and your family: https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/securing-home-network/

In the News

Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn



(Becky Bracken | March 31, 2022)

A bug in Honda is indicative of the sprawling car-attack surface that could give cyberattackers easy access to victims, as global use of 'smart car tech' and electric vehicles (EVs) surges.

A pair of recent vulnerabilities found in the automaker ecosystem might not seem like a real danger taken separately. But experts warn a lack of attention on cybersecurity could plague "smart" car and electric vehicle systems — and users — in years to come, as the use of automotive technology continues to explode.

One bug was recently found in the communications between the remote keyless entry function on Honda and Acura cars.

Easily intercepted radio signals from the wireless entry key fob on almost any Honda and Acura vehicle could allow a threat actor to lock and unlock, and even start the car, according to a new disclosure from a pair of researchers.

Ayyappan Rajesh, who is a student at UMass Dartmouth, and Blake Berry (HackingIntoYourHeart) reported the flaw (CVE-2022-27254) and provided additional details of the vulnerability in a GitHub post.

"A hacker can gain complete and unlimited access to locking, unlocking, controlling the windows, opening the trunk, and starting the engine of the target vehicle where the only way to prevent the attack is to either never use your fob or, after being compromised (which would be difficult to realize), resetting your fob at a dealership," the post said.

All the attacker needs to takeover the car is a recording of the unencrypted commands sent from the fob, the post added.

Full Story: https://threatpost.com/automaker-cybersecurity-lagging-tech-adoption/179204/

A Few More Cyber News Stories:

Google: Multiple hacking groups are using the war in Ukraine as a lure in phishing attempts
https://www.zdnet.com/article/google-multiple-hacking-groups-are-using-the-war-in-ukraine-as-a-lure-in-phishing-attempts/

Ransomware Payments Hit New Records
https://cyware.com/news/ransomware-payments-hit-new-records-db1d27d8

82% of Public Sector Applications Contain Security Flaws
https://www.infosecurity-magazine.com/news/public-sector-apps-security-flaws/

CYBER CHALLENGE

Why So Serious?

This Month's Challenge

For this month's challenge, let's see your best security awareness meme! Time to turn that awareness training into a visual we can grasp.

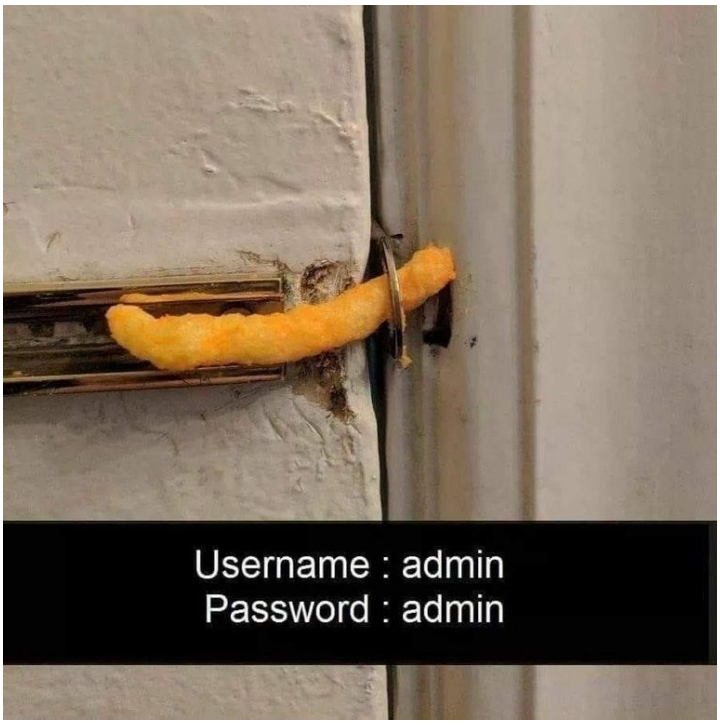
We all know cyber security is serious business. But that doesn't mean we can't have a few laughs with some nerdy amusement.

The challenge breakdown:

- Scour the internet for (work-appropriate) memes with a security awareness takeaway which also makes you laugh….or smile, at least.
- Share your best few with me, and I'll pick my favorites to share next month.
- Bonus points if you create your own meme! But please use a personal device for those meme-generating websites and be mindful when perusing the Internet with a work-issued device.

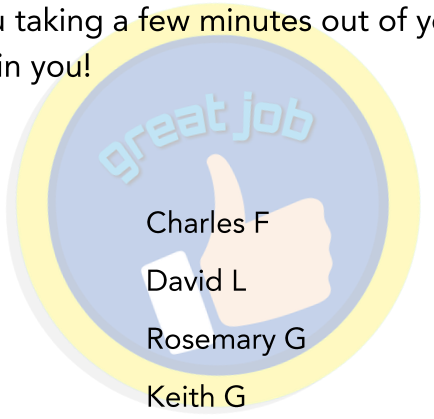
Here's one of my all-time favorites. Come on, you giggled. (Just me?)

Your turn! Let's have some fun!



Closing Comments

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to try the last cyber challenge! We fully appreciate you taking a few minutes out of your day to engage with us! Please keep doing so; and get others to join you!



A big THANK YOU to:

Alicia P	Menrose M	Charles F
Wendy W	Susan W	David L
Caroline A	Colleen A	Rosemary G
Matthew M	SJ J	Keith G
Vikki G	Rita G	Allison M
Steven C	Susan M	
Aaron W	Lance J	

If we missed you, let us know!

Last month, a DPS colleague of ours in the Houston region sent me an intriguing story she picked up in a forum of communication dispatch groups. And I'm so glad she did!

I didn't listen to the podcast (please feel free to with the link below), but I read the transcript and couldn't believe what I was reading happened in real life.

As you can imagine, there's lots an angry person can do with the information they can find about you on the web. This story starts with a seemingly harmless prank of having pizza delivered to this guy's house unexpectedly….and escalates to using his information to dial 911 and have a SWAT team arrive at his front door fully armed and expecting imminent danger.

I won't ruin it for you, but it's worth the lengthy read/listen (there are a few colorful words so fair warning). Let me know what you think! And please send me stuff like this; I really enjoy it.

Darknet Diaries: https://darknetdiaries.com/transcript/106/

Thank you for all you do, and thank you for your continued cyber diligence!

Share and Connect

Newsletter Archive Cyber SharePoint