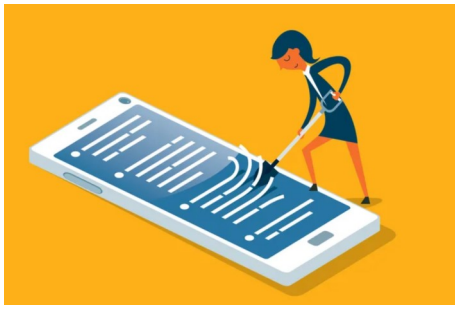
CYBER SECURITY NEWS
Vol. 7 | Issue 5
May 2022

Welcome to the TXDPS Cyber Security Newsletter!

Via CNET

It's likely your personal information is available to the public; "public" meaning everyone, everywhere.



It's never a bad time to get your internet privacy ducks in a row and effectively "delete" yourself from the internet. (If you're wondering how deleting yourself from the internet can stop companies from getting hold of your info? Short answer: It can't.)

You can never completely remove yourself from the internet, but there are ways to minimize your digital footprint, which would lower the chances of your personal data being out there.

Here are some ways to disappear your digital self:

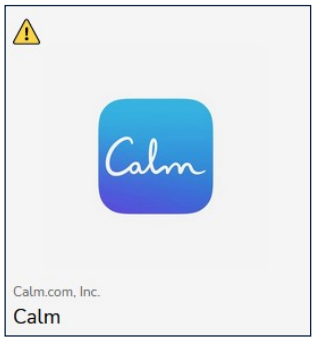
- Delete or deactivate your shopping, social media and web service accounts.
  - Think about which networks you have social media profiles on. Also, which shopping sites have you registered on?
- Remove yourself from data collection sites
  - There are companies out there that collect your information. They're called data brokers, and they have names like Spokeo, Whitepages.com and PeopleFinder, as well as plenty of others. How to opt out of each site varies.
- Remove your info directly from websites
  - Check with your phone company or cell provider to make sure you aren't listed online and have them remove your name if you are. If you want to remove an old forum post or an old embarrassing blog you wrote back in the day, you'll have to contact the webmaster of those sites individually.
- Remove your email accounts
  - You'll have to sign into your account and find the option to delete or close the account. Some accounts will stay open for a certain amount of time if you want to reactivate them.
  - An email address is necessary to complete the previous steps, so make sure this one is your last.

Remember to be patient when going through this process, and don't expect to complete it in one day. You may also have to accept that there are some things you won't be able to permanently delete from the internet.

More details on how to remove your digital footprint: https://www.cnet.com/tech/services-and-software/your-private-data-is-all-over-the-internet-heres-what-you-can-do-about-it/

In the News

Mozilla finds mental health apps fail 'spectacularly' at user security, data policies



(Charlie Osborne | May 2, 2022)

An investigation into mental health and prayer apps has revealed a disturbing lack of concern surrounding user security and privacy.

On Monday, Mozilla released the findings of a new study into these types of apps, which often deal with sensitive topics including depression, mental health awareness, anxiety, domestic violence, PTSD, and more, alongside religion-themed services.

According to Mozilla's latest *Privacy Not Included guide, despite the deeply personal information these apps manage, they "routinely share data, allow weak passwords, target vulnerable users with personalized ads, and feature vague and poorly written privacy policies."

In a study of 32 applications geared toward mental health and religion, the organization found that 25 of them did not meet Mozilla's Minimum Security Standards.

These standards act as a benchmark for the *Privacy Not Included reports. The mismanagement or unauthorized sharing and sale of user data, vague data management policies, a lack of encryption, weak password policies, no clear vulnerability management system, and other lax security policies can all downgrade a vendor product in the eyes of Mozilla.

If an app or service fails to meet these basic requirements, they are slapped with the "*Privacy Not Included" warning label.

The mental health and prayer-related apps have received an accolade -- but not one you'd covet.

The company says: "When it comes to protecting people's privacy and security, mental health and prayer apps are worse than any other product category Mozilla researchers have reviewed over the past six years."

Full Story: https://www.zdnet.com/article/mozilla-finds-mental-health-apps-fail-spectacularly-at-user-data-security/

A Few More Cyber News Stories:

Bad Actors Are Maximizing Remote Everything
https://threatpost.com/bad-actors-remote-everything/179458/

U.S. DoD tricked into paying $23.5 million to phishing actor
https://www.bleepingcomputer.com/news/security/us-dod-tricked-into-paying-235-million-to-phishing-actor/

T-Mobile Secretly Bought Its Customer Data from Hackers to Stop Leak. It Failed.
https://www.vice.com/en/article/k7w9mv/tmobile-hacked-bought-data-mandiant

CYBER CHALLENGE

Football Fever

This Month's Challenge

For this month's challenge, let's play a football-themed game putting cyber awareness training to the test!

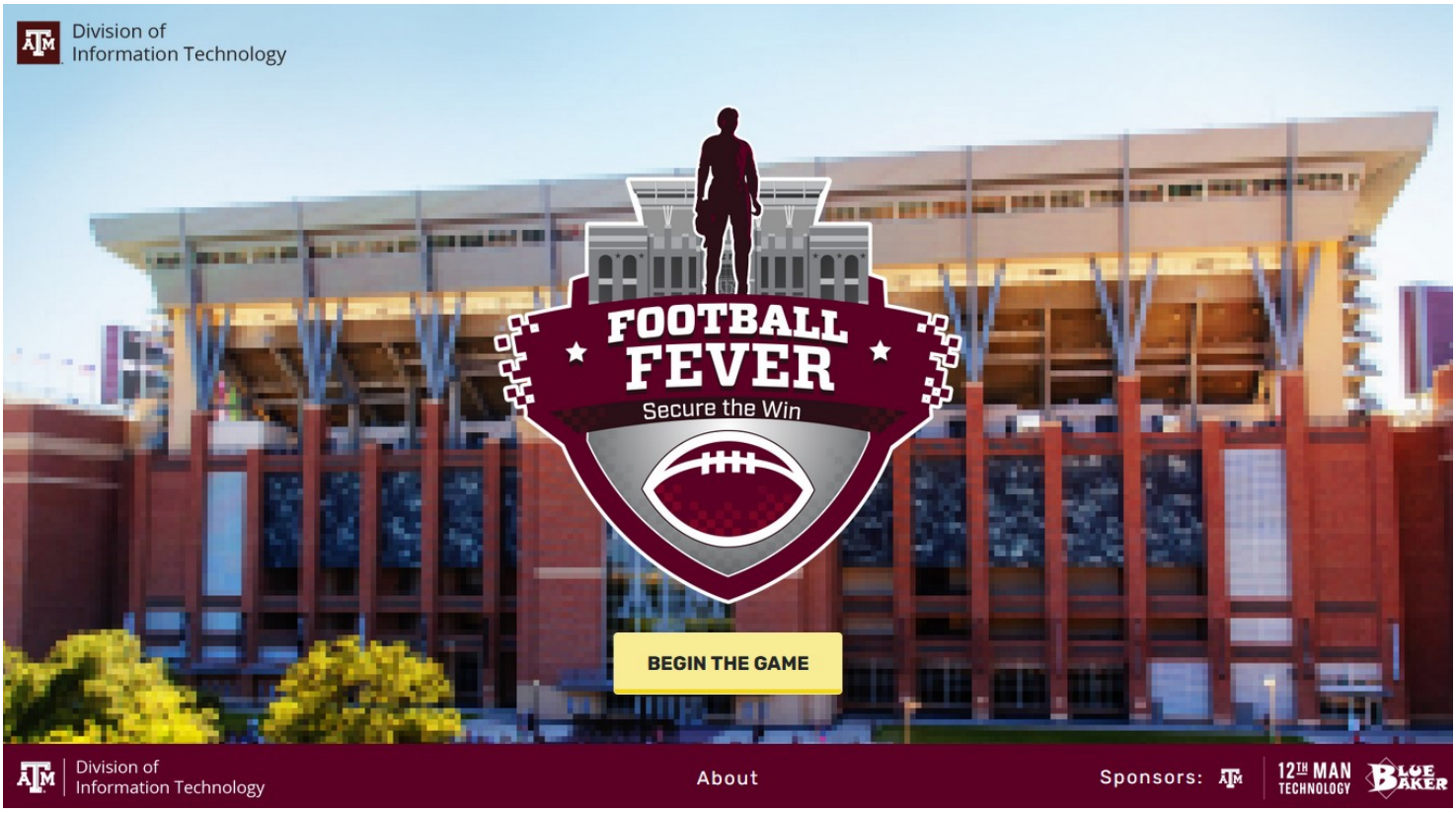
Texas A&M's IT Division creates cyber security games every year, and most of them are great! Well...you know...for a group of Aggies.

I kid, I kid! Please hold the hate mail. These games are always awesome.

Let me know what your final score is. Hopefully you secure the win! (~10 min. to complete)

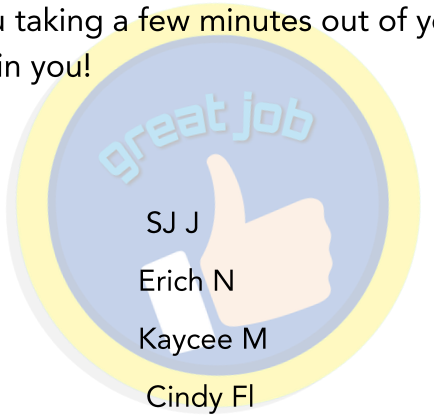
Good luck!

https://it.tamu.edu/footballfever/



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:

Kari R	Mark F	SJ J
Vikki G	Michele R	Erich N
Liliana A	Wendy S	Kaycee M
Allonia N	Richard Z	Cindy Fl
Stephanie H	Christine S	
April T		

Keep scrolling for my favorite memes. It was so hard to pick! Thanks for the laughs!
If we missed you, let us know!

Maybe it's the nerd in me (it obviously is), but I love me a cool cyberthreat map.

There are many out there if you're interested enough to look them up. I thought I'd share a few of my favorite.

These maps show cyber attacks in real-time. Many of them show the type of attack as well as the attacking country and the target country.

At the very least, the colors and animations are neat! (Nerd alert!)

Fortinet: https://threatmap.fortiguard.com/
Bitdefender: https://threatmap.bitdefender.com/
SonicWall: https://securitycenter.sonicwall.com/m/page/worldwide-attacks

Thanks for the read; and thank you for all you do. Stay safe out there!

- Eric Posadas


MULTI-MILLION CORPORATE CYBER SECURITY SPENDING
USER WITH LOCAL ADMIN RIGHTS OPENS EMAIL ATTACHMENT


I CHANGED ALL MY PASSWORDS TO "INCORRECT"
SO WHENEVER I GET THE PASSWORD WRONG, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT"!!


YOU SAID MFA WOULD PROTECT US!
THEY USED A MALICIOUS O365 APP!
I HAVE NO IDEA WHAT THAT MEANS!
WHY DO YOU CLICK ACCEPT ON EVERYTHING!
YOU SAID DONT GIVE OUT YOUR PASSWORD! IT DIDN'T ASK FOR A PASSWORD!


FACEBOOK NOW HIRING.
NO NEED TO APPLY.
WE ALREADY HAVE ALL YOUR DETAILS


SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.


WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick


SECURITY OPTIONS
PASSCODE TO UNLOCK SET CODE
ERASE PHONE AFTER TEN FAILED UNLOCK ATTEMPTS
IF STOLEN, PHONE CAN BE REMOTELY
TRACKED
ERASED
DETONATED
IF PHONE IS STOLEN, ERASE DATA AND PLAY AN EARSPLITTING SIREN UNTIL THE BATTERY DIES OR IS REMOVED
IF PHONE IS STOLEN, DO A FAKE FACTORY RESET. THEN, IN THE BACKGROUND...
...CONSTANTLY REQUEST DOZENS OF SIMULTANEOUS RIDESHARES TO THE PHONE'S LOCATION
... AUTOMATICALLY ORDER FOOD TO PHONE'S LOCATION FROM EVERY DELIVERY PLACE WITHIN 20 MILES
... IF THIEF LOGS IN TO FACEBOOK, SEND HOSTILE MESSAGES TO ALL THEIR FAMILY MEMBERS
... AUTOMATICALLY DIRECT SELF-DRIVING CAR TO DRIVE TOWARD PHONE'S LOCATION AT 5 MPH
...TAKE PHOTOS OF RANDOM OBJECTS AT THE THIEF'S ADDRESS AND POST THEM AS "FREE" ON CRAIGSLIST AND NEXTDOOR


ILL MAKE THEM DO CYBER AWARENESS TRAINING
AND THEN
ILL MAKE THEM DO IT AGAIN AND AGAIN