CYBER SECURITY NEWS

Vol. 5 | Issue 11

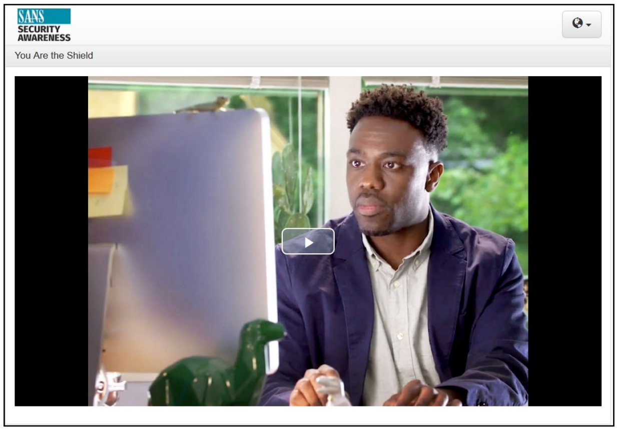
December 2020

Welcome to the TXDPS Cyber Security Newsletter!

We hope you had a safe, fulfilling Thanksgiving break, and we send you our warmest wishes as we continue through the holiday season and make our way toward 2021.

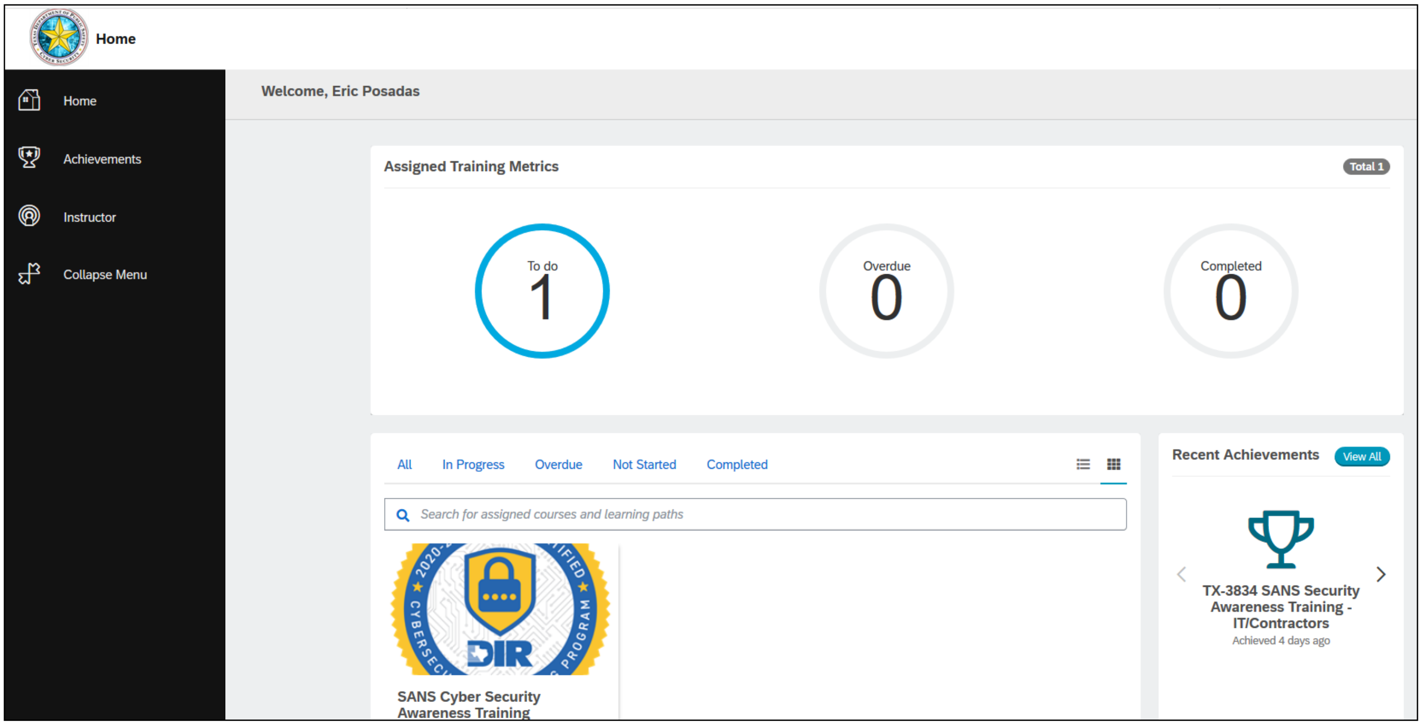
Speaking of 2021, we are excited to announce that we will be moving our cyber security awareness training to a new platform in the new year!

Our cyber security awareness training vendor, SANS, has moved to the Litmos learning platform. Much of the content has been refreshed, and the new design with a more modern aesthetic is a very welcomed update.



We will provide more information and instruction once we get closer to our transition. For now, please make sure you've completed your annual cyber awareness training before the end of the year. I will be sending a reminder message to those of you who have yet to complete it so if you receive a message from me, I urge you to finish up the training so you don't have to start over once we move to the new system.

Aren't sure of your completion status? If you haven't heard from me recently, you're probably good to go but feel free to shoot me a message, and I'd be happy to check for you.



Welcome, Eric Posadas

Assigned Training Metrics — Total 1

To do 1

Overdue 0

Completed 0

SANS Cyber Security Awareness Training

Recent Achievements

TX-3834 SANS Security Awareness Training - IT/Contractors

Achieved 4 days ago

Cyber Risk Management

"Dance like no one is watching, encrypt like everyone is." - Werner Vogels, Amazon's Chief Technology Officer

What a great piece of advice. In fact, spotting this quote on a t-shirt recently inspired this month's look at a cyber security control – encryption.

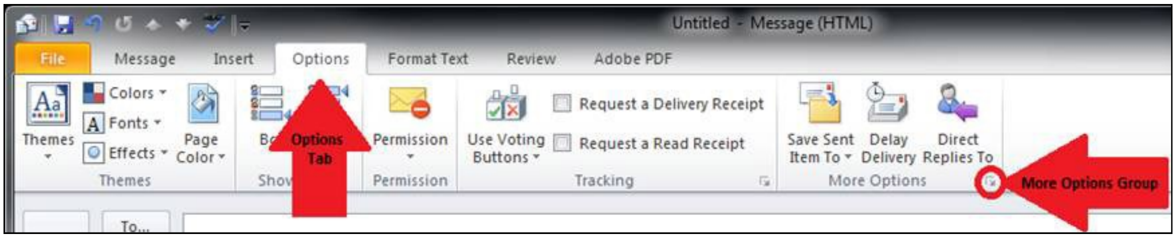
Encryption is the process of altering a piece of information so that only the intended receivers can understand it. While this may sound complex, it is a fairly straightforward concept. An extremely simplistic analogy found in a tech blog states: "Imagine you want to communicate with another person in the room, sharing a vocal message that a third person in the room won't understand. If the three of you can speak English, but only you and your receiver can speak French, you would "alter" your message to French. You formulate your thought in English, but say it in French. This way, only the other person speaking French will understand it." Of course, for encryption to be secure, only the intended receiver must understand (or "decrypt") the message, and no one else.

Encryption is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet. For example, many websites and other online services encrypt data transmissions over the web. Any website that begins with "https://" uses the HTTPS protocol, which encrypts (and protects) all data sent between the web server and your browser. Quick side note: you should look for this "https" on websites while shopping online this holiday season.

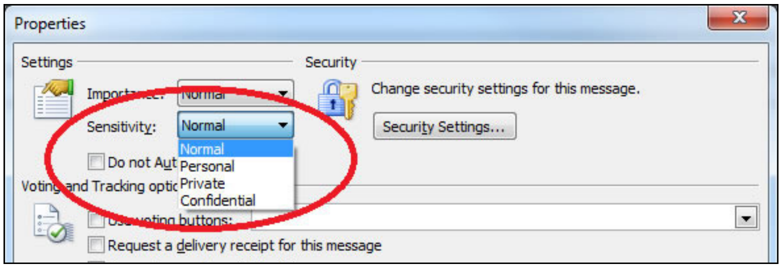
One way you might directly interact with encryption is through email. When using email to send sensitive or confidential information, email encryption is used to protect that data from being read by an outside party. As a DPS employee, be sure to encrypt any email containing sensitive/confidential information to outside entities, in accordance with the General Manual, Chapter 26.110.00, addressing proper email use. Doing so will greatly increase our security posture and help us keep DPS data from being read by malicious actors.

Here's how to encrypt DPS email before sending:

1. Open Outlook and create a new email message. Click on the "Options" tab and then click on the small arrow in the "More Options" group.



2. In the "Properties" window that appears, select "Confidential" in the "Sensitivity" field. Then click on the "Close" button at the bottom of the Properties window. You can now compose and send your encrypted email message.


Importance: Normal

Sensitivity: Normal

Properties
Settings
Security
Change security settings for this message.
Security Settings...
Normal
Personal
Private
Confidential
Do not Aut
Voting and Tracking optic
Use voting buttons:
Request a delivery receipt for this message

Your Info is Breached, Now What?

It’s hard to avoid hearing about data breaches these days – and unfortunately, it’s almost as hard to avoid being affected by them. A “data breach” is any event in which data that’s supposed to be private is exposed to unauthorized viewers. For example, a database full of personal information about individuals, including names, contact information, passwords, identifiers such as social security numbers, credit card data, and/or personal health data we’d rather the whole world didn’t know about.

These days, many online services require us to provide at least some of our personal information, ranging from our names and phone numbers to more sensitive data like our credit card numbers or login information. We typically supply this information and trust the companies and websites we use to keep them safe. But, as we all know, that doesn't always happen. In fact, it’s highly likely some of your own information has been caught in a data breach and is for sale on the dark web right now. (If you somehow evaded the Experian credit bureau breach that caught 147 million Americans, the Target breach that caught 110 million shoppers, the Adobe breach of 156 million accounts, the Home Depot breach of information on 56 million payment cards, and the Facebook breach of over 540 million user records, you’re one lucky person!) In all seriousness, these are a big deal, and if you haven’t been caught yet, it’s probably just a matter of time.

So..how can you protect yourself from a data breach?

- **Be preemptive**. Monitor your accounts closely and look at your account’s privacy settings.
- **Use strong passwords**, especially on financial accounts. And, use different passwords across different websites and services. A password keeper will help manage these.
- **Limit what you share** on social media. Cybercriminals use this info to answer security questions.
- **Avoid public Wi-Fi**, such as those found at coffee shops.

Unfortunately and frustratingly, even if we do our best to protect our information, sometimes the companies we trust are breached, and our info gets out despite our due diligence.

So...what do you do after you learn your data’s been breached?

- **Get confirmation.** Avoid scams by going to the company’s website or call to confirm. You can also use “https://haveibeenpwned.com/” (it looks scammy, but it’s legit) to learn if your information has been exposed. That website also allows you to sign up for email alerts in case another breach occurs.
- **Figure out what was exposed**. Understanding which information was exposed will help determine your next steps.
  - If your credit card info was stolen, notify your bank and request credit freezes with all three credit bureaus.
  - If your social security number has been compromised, notify the IRS and Federal Trade Commission. identitytheft.gov
- **Find immediate help**. See if the company is offering help in the form of monetary assistance, credit monitoring, or other recovery services.
- **Change your passwords**. This obviously won’t help recover your breached info, but it will help protect further information from being exposed.
- **Consider purchasing identity theft insurance**. While this doesn’t guarantee against theft, it provides monitoring to minimize serious consequences and may include financial assistance.

It’s hard not to feel helpless with data breaches. But while you many not be able to control many of them, you can be proactive and keep your data as secure as possible.

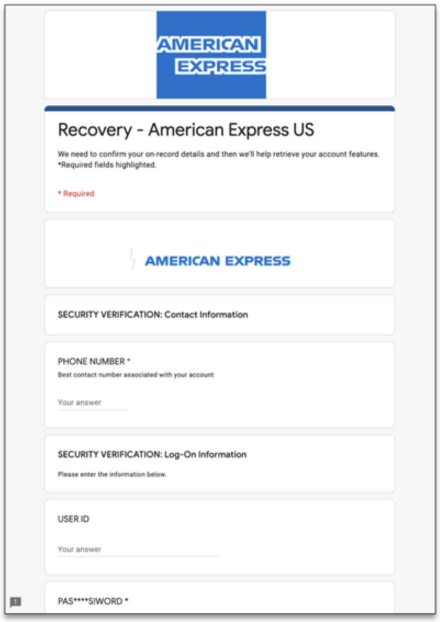
In the News

Google's Free Services and Phishing Campaigns: A Likely Pair

(Stu Sjouwerman | November 19, 2020)

Cybercriminals are now launching phishing campaigns that abuse Google's free productivity tools while also using social engineering to trick you into installing malware.

Some of Google's free offerings range from documents, spreadsheets, online forms, and free websites. These tools are primarily used by the education sector, which can be an easy target for the bad guys to infiltrate. A new report released by email security firm ArmorBlox showed how the bad guys are creating these elaborate campaigns that look convincing but avoid any detection of a scam.



Recovery - American Express US

We need to confirm your on-record details and then we'll help retrieve your account features.
*Required fields highlighted.

* Required

SECURITY VERIFICATION: Contact Information

PHONE NUMBER *
Best contact number associated with your account
Your answer

SECURITY VERIFICATION: Log-On Information
Please enter the information below.

USER ID
Your answer

PAS****SIWORD *

American express phishing form on Google Forms
Source: ArmorBlox

In this example, threat actors are abusing Google Forms to steal your credentials.

To protect our agency (and yourselves at home) from these types of attacks, it's important to observe subject-sensitive emails, especially when it's related to money. Treat all email that have links and/or attachments as suspicious, and report any unsuspecting email to our security team. *Bleeping Computer* has this full story on their website.

Full Story: https://www.bleepingcomputer.com/news/security/google-s-free-services-are-now-phishing-campaign-s-best-friends/

A Few More Cyber News Stories:

Twitter names famed hacker 'Mudge' as head of security
https://www.reuters.com/article/us-twitter-security/twitter-names-famed-hacker-mudge-as-head-of-security-idUSKBN27W2MB

After years of work, Congress passes 'internet of things' cybersecurity bill - and it's kind of a big deal
https://www.cyberscoop.com/congress-iot-cybersecurity-bill-contractors/

Facebook Messenger Bug Allows Spying on Android Users
https://threatpost.com/facebook-messenger-bug-spying-android/161435/

CYBER CHALLENGE

Spot the Fake Face

This Month's Challenge

As technology and machine learning continue to advance so does the ability to push disinformation. It's steadily become easier to alter videos of actual footage to create a lie, produce fake audio that sounds exactly like the targeted person, and to create faces for portraits of a person who doesn't even exist.

Generative adversarial networks (GANs) are an exciting innovation in machine learning. But just like any technology, this tool can be used maliciously to sow discord.

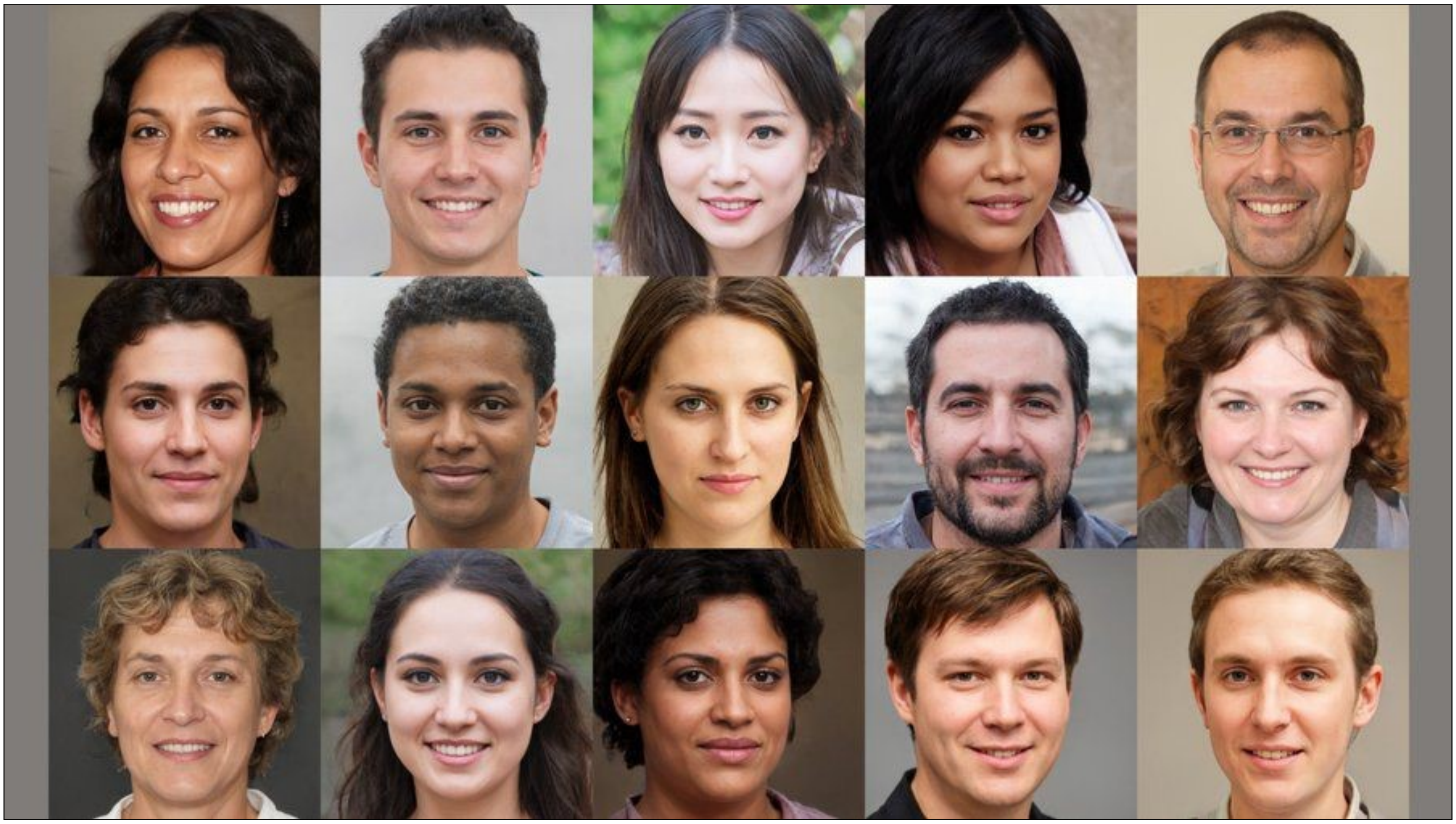
Among the many uses and abilities, GANs can create images that look like photographs of human faces, even though the faces don't belong to any real person.

This month, let's test your eyes with the ability to spot a portrait generated by artificial intelligence software. Which one of the pictures below is of a fake person? Are you able to spot the disinformation?

Take a look at this gallery, and once you've figured out which one of these isn't a real person, let me know, and I'll let you know how sharp your eyes are.

Hint: Squinting may help.

Good luck!



</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 play the cyber awareness game from Living Security after last month's newsletter was published! We fully appreciate you taking a few minutes out of your day to engage with us!

A big THANK YOU to all who emailed us!

I'd like to reiterate one more time it's Holiday Season for the bad guys, too! But not the way you might think. They go into scam-overdrive mode. We are in the middle of the busiest online shopping days, and the bad guys are planning to get rich with your money.

So, here are this year's **Top 10 Holiday Cybersecurity Alert Tips** from our friends at KnowBe4:

- Keep all devices up to date with basic security measures to lessen your chance of becoming the victim.
- Only connect to known Wi-Fi networks
- Use strong, unique passwords on all accounts. This is a good time to update passwords!
- Be safe on all social media; don't overshare and take the time to review your privacy settings on the platforms you use.
- Keep an eye on your bank accounts and monitor your credit report regularly.
- Be careful with messages regarding shipping changes. Always use official channels to stay updated.
- Watch out for holiday greeting cards that may not be the sender you think! Don't open these unless you're certain you can trust who they came from.
- Keep devices in view (or know where they are) throughout the course of all holiday travel.
- Pay close attention to the websites you visit and shop on. It's safest to only use those you trust.
- Be wary of ads, giveaways, and contests that seem too good to be true. These run rampant during the holiday season!

You can download the tip sheet here to share with your friends and family as well.

Thank you for swinging by and checking out this month's newsletter! And, as always, thank you for your cyber vigilance! Happy holidays!

- Eric Posadas