TEXAS A&M UNIVERSITY

POSSIBILITIES

FALL 2018 Division of Information Technology

ABOUT THIS ISSUE

In recognition of National Cyber Security Awareness Month, this issue is devoted to tips and stories to help you stay safe online.

We invite you to brush up on security terminology and awareness and then test your knowledge with our online game, "Aggie LIFE."

You can always find great security tips at **security.tamu.edu**.

Don't forget to tell us what you think about this newsletter at **tamu-it-coms@tamu.edu**.

CYBER SECURITY AWARENESS MONTH

Don't Let (Aggie) LIFE Pass You By

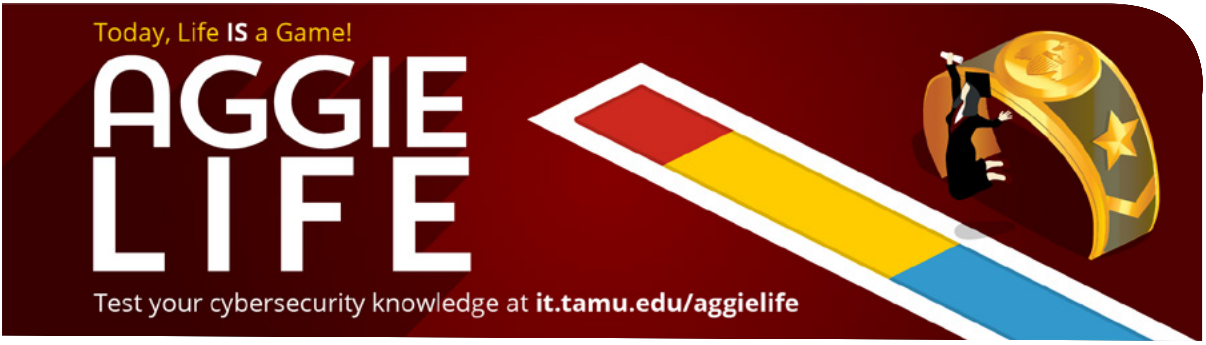
A cyber threat isn't a game, but testing your cybersecurity smarts can be!

As part of National Cyber Security Awareness Month, the Division of Information Technology invites you to play Aggie LIFE! This isn't a board (or boring) game, it's an online journey that begins at Texas A&M and continues onward to a successful career.

Complete the game between October 15-26 to receive your choice of either a FREE five-ounce frozen yogurt from Yogurtland, a day of play at Nerdvana Vintage Arcade and Toys, or a 12th Man Towel from Aggieland Outfitters.

The player with the highest score wins an Apple Watch, so play as many time as you want.

To play, go to **it.tamu.edu/aggielife**.



DON'T GET HOOKED

How to Tackle Phishing Attempts

Think you're careful enough not to get "reeled in" by a phishing attempt? Believe it or not, statistics show 30 percent of all phishing emails get opened!

Just like a good lure, some phishing emails look authentic and often contain convincing logos, legitimate phone numbers and email signatures from actual employees. So here are some things to look for so you don't become the "catch of the day":

Too good to be true

Criminals know the best bait includes offers of money, free stuff and other goodies. Recent campus attempts claimed recipients were eligible for tuition refunds.

Threats

Another favorite lure in the phisher's tackle box involves threats! These may be warnings of an account closing, possible legal action, etc. to force hasty decisions.

Immediate action required

Fraudulent emails use urgency, which can lead to hasty decisions. Think before you click.

Impersonal

Companies and major entities make an effort to address you personally when action is required. Phishing attempts, however, often use greetings such as "Dear User."

Poor spelling and grammar

Bad grammar and spelling errors are telltale signs of a phishing attempt. Government entities, universities and companies proof messages before they are distributed.

Check the line

Scammers hide fake URLs in real-looking hyperlinks. When you click a link to what you think is one website, it takes you to a scam website. Always hover over links to see where they really lead.

Who's it from?

Scammers use legitimate-looking email addresses to trick you into thinking an email is real. Beware of "from" addresses such as support@wlsfrgo.com that seem real, but aren't.

The university community is a "big pond" for scammers, so stay vigilant as you check your email inbox! If you receive a suspicious message, contact Help Desk immediately at helpdesk@tamu.edu or 979.845.8300.

Division of IT Hosts Cybersecurity Showcase

Hear from world-renowned security pros during the Division of IT's Cybersecurity Showcase, October 19 at the Texas A&M Hotel & Conference Center.

The event is free for Texas A&M students and employees, but seating is limited. Sign up at **https://bit.ly/2OjnQVl**

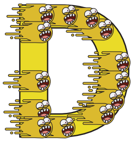
KNOW THE LINGO

The ABCs of Cybersecurity

To understand cyber threats, it helps to know all of the terms involved. Below is a non-exhaustive (yet exhausting) list you should know:

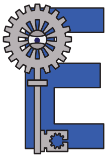
Cookie

While the word "cookie" usually refers to sugary dessert treats, browser cookies aren't always sweet! Cookies refer to the data servers send to a web browser to keep track of visits. While cookies can be helpful, they can also be used to disguise malware or track your online activity.



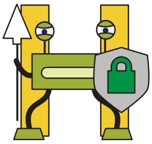
Denial of Service (DoS) Attack

This just sounds scary, and it is. To shut down large networks or websites, these attacks flood the target with traffic. Music services, social media sites and others are often targets.



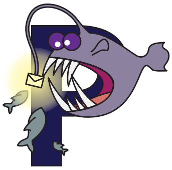
Encryption

Let's skip the 0s and 1s and just say encryption is the process of converting data (called plaintext) into a code (called ciphertext") to prevent unauthorized access.



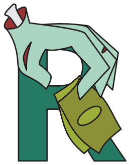
Https

In the address bar of your browser, the portion before the colon is usually http or https. The "s" stands for secure and means the site should be safe.



Phishing

These emails appear to be from reputable companies and try to trick users into revealing personal info such as credit card numbers or login information.

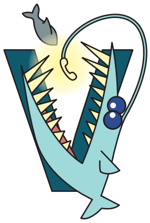


Ransomware

Nasty malware that encrypts the hard drive of a victim's computer and holds the data "hostage" until a ransom is paid out. Unfortunately, payment doesn't guarantee your data will be released.

Social Engineering

This is the practice of tricking people into willingly giving out personal or confidential information.



Vishing

In this phone equivalent of phishing, the scammer calls their victims in an attempt to make them release private info used for identity theft.

Worms

These creepy crawlers are malicious programs that can run independently and are designed to infect other computers while remaining active on infected machines. Antivirus programs and firewalls are the best ways to prevent infection.

Want more? Download our full A-Z poster at
u.tamu.edu/cyber-abcs.

JUST DUO IT

When it Comes to Security, Two is Better than One

Texas A&M University is adding a second layer of security with Duo NetID Two Factor Authentication, a service that will soon be required for the entire campus community. So what is two-factor authentication and how will it protect you?

Since usernames and passwords are vulnerable, two-factor authentication takes an additional step to verify the user is whom they say they are by requiring something they know (the username and password) and something they have (such as a mobile device or a hardware token). When you sign up for Duo, you can have the system call your mobile device or landline, or send an authentication request to your Duo app.

The following campus groups will be Duo-required by the dates indicated:

- **October 15, 2018:** All U1 students
- **October 30, 2018:** All campus IT professionals
- **May 15, 2019:** All Texas A&M University employees

To learn more about enrolling in Duo, visit **duo.tamu.edu**.

Alexa Arrives at Texas A&M

Does all this cybersecurity talk make you want to change your NetID password, but you're not sure how? Need directions to Help Desk Central? Simply ask Amazon Alexa using the new "Aggie Tech Help" skill from the Texas A&M Division of Information Technology.

Users on campus can access Aggie Tech Help using the Alexa app on a mobile device. The skill will also work off campus on Amazon devices such as the Echo and Dot. Just say, "Alexa, enable Aggie Tech Help."

More information and instructions for using Aggie Tech Help can be found at **it.tamu.edu/alexa**. The skill and additional instructions are at **amazon.com/alexaskills**.

Division of Information Technology
3142 TAMU | College Station, TX | **IT.tamu.edu**