Information Technology Division Bulletin
vol. 17 no. 2 | October 2020

We Are All Responsible
Cybersecurity Awareness Month Special Edition

Message from the CIO

The National Cybersecurity Alliance designates October as "National Cybersecurity Awareness Month." Texas Tech University has participated in this initiative since its inception in October 2004. Given the current pandemic, the TTU IT Division will host a number of online educational activities for faculty, staff, and students, instead of our usual face-to-face events. Preying on COVID-19 fear and anxiety, cyber-criminal activity has proliferated beyond expected in 2020 (INTERPOL Report, August 4, 2020). We are challenged to match this insurgence with heightened vigilance. To that end, we encourage the TTU Community to review the materials provided in this issue in order to help protect TTU information resources and data. Note that many of these tips will also help you protect your personal devices and data. Your partnership is critical in protecting institutional assets and information. Go Tech!

—Sam Segran, Chief Information Officer and Vice President for IT

INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19

(INTERPOL, August 4, 2020), INTERPOL report shows alarming rate of cyberattacks during COVID-19, *reprinted in full accordance with INTERPOL informational and public awareness purpose policy, copyright INTERPOL.*

An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure.

With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits, and cause disruption.

In one four-month period (January to April), some 907,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners.

> *"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."*
>
> Jürgen Stock, INTERPOL Secretary General

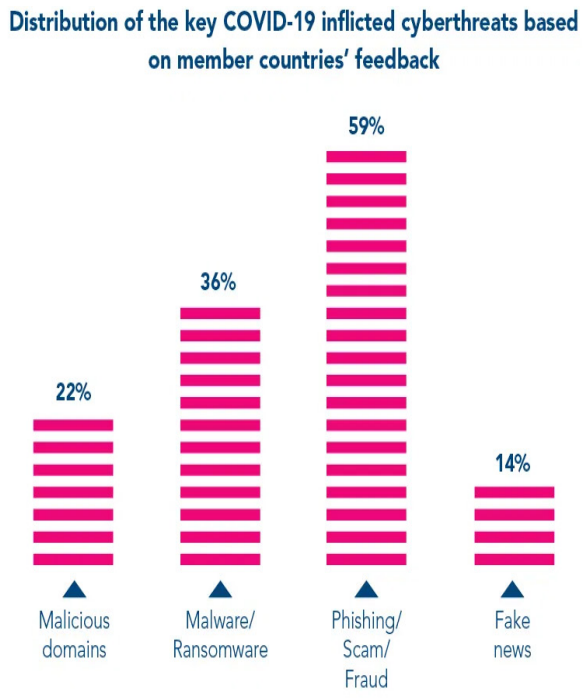
"The increased online dependency for people around the world, is also creating new opportunities, with many businesses and individuals not ensuring their cyber defenses are up to date."

"The report's findings again underline the need for closer public-private sector cooperation if we are to effectively tackle the threat COVID-19 also poses to our cyber health," concluded the INTERPOL Chief.

Key findings highlighted by the INTERPOL assessment of the cybercrime landscape in relation to the COVID-19 pandemic include:

- Online Scams and Phishing - Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content. Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.
- Disruptive Malware (Ransomware and DDoS) - Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit. In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months. Law enforcement investigations show the majority of attackers estimated quite accurately the maximum amount of ransom they could demand from targeted organizations.
- Data Harvesting Malware - The deployment of data harvesting malware, such as Remote Access Trojan, info stealers, spyware, and banking Trojans, by cybercriminals is on the rise. Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money, and build botnets.
- Malicious Domains - Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords such as "coronavirus" or "COVID." These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment, and phishing. From February to March 2020, a 569% growth in malicious registrations, including malware and phishing, and a 788% growth in high-risk registrations were detected and reported to INTERPOL by a private sector partner.
- Misinformation - An increasing amount of misinformation and fake news is spreading rapidly among the public. Unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks. Nearly 30% of countries which responded to the global cybercrime survey confirmed the circulation of false information related to COVID-19. Within a one-month period, one country reported 290 postings with the majority containing concealed malware. There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities. Other cases of misinformation involved scams via mobile text-messages, containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets.

Continued: INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19



Projections
Future primary areas of concern highlighted by the INTERPOL report include:

- A further increase in cybercrime is highly likely in the near future. Vulnerabilities related to working from home and the potential for increased financial benefit will see cybercriminals continue to ramp up their activities and develop more advanced and sophisticated modi operandi.
- Threat actors are likely to continue proliferating coronavirus-themed online scams and phishing campaigns to leverage public concern about the pandemic.
- Business Email Compromise schemes will also likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activities.
- When a COVID-19 vaccination is available, it is highly probable that there will be another spike in phishing scams related to these medical products as well as network intrusion and cyberattacks to steal data.

Beware of Scams Appearing to Come from Senior Texas Tech Administrators

Cyber criminals are always looking for new ways to steal your identity or scam you into sending them money. Recently, scammers have begun impersonating Texas Tech administration, such as the Chancellor, President, Deans, and Department Heads, to trick readers into providing their personal information. These messages typically have the following elements in common:

1. Purport to come from a Texas Tech administrator in the Display Name but are sent from non-TTU email addresses (such as aol.com or gmail.com). You can determine the actual email address of a sender in the following ways:

- Outlook: Open the message, then right-click the sender name and select «Open Contact Card» (PC) or «Open Outlook contact» (macOS);
- Outlook on the Web: Open the message, then hold your mouse pointer over the sender name for 2-3 seconds;
- Mobile Clients: Open the message, then tap the sender name.

2. Begin with a subject, such as "Quick Request" or "Are you available," with a message body of "Available?" Some messages may say they are in a meeting where phone calls are not allowed.

3. If the recipient responds, the scammer may ask for the recipient's cell phone number. Another variant states that they would like to surprise their staff with gift cards and asks the recipient to buy them on their behalf and provide the card numbers electronically.

Most of these are automatically caught by TechMail's Advanced Threat Protection, but if you are concerned about a message's authenticity, please contact IT Help Central for further assistance. If you receive one of these, or similar messages, please contact IT Help Central immediately at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu. Do not respond to these messages or click any links within them. Please note that the IT Division is currently exploring options to flag emails that come from outside the ttu.edu domain so that recipients will have additional information to protect themselves.

We encourage you to practice cybersecurity and to be aware of activities designed to steal institutional and personal resources. You can find images of these and other scams online at http://www.askit.ttu.edu/phishingexamples.

For more information or if you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Protecting Personal and Institutional Data

As the need for learning, teaching, and working remotely continues, the TTU IT Division strongly recommends that faculty, staff, and students be vigilant in protecting institutional and personal data and information resources.

The TTU IT Division has the following measures in place to protect confidential and sensitive data:

- 2-Factor Authentication: Prevents unauthorized account access by sending a code to the account owner when their account is accessed from a new location.
  Note: 2-Factor Authentication is currently enabled on Texas Tech's Direct Deposit, eRaider Account Manager, Banner 9 Admin, and W-2 Wage and Tax Statement pages. You can enable this feature for all eRaider-authenticated pages by following the instructions at askit.ttu.edu/2fa.

- Symantec Endpoint Protection: Capable of detecting and removing most keylogger software and malware. You may download Symantec at no cost by visiting eraider.ttu.edu, selecting "Manage Your Account," and then choosing "Software Download" on the left menu.

- Microsoft Advanced Threat Protection: ATP checks links and attachments contained in all incoming email to determine if they are malicious.

Additional information about ATP:

In an effort to protect users from malicious websites, links will appear slightly different:

- Links will be prepended with "https://na01.safelinks.protection.outlook.com/?url=" when you hold your mouse pointer over them.

- When you click a link, the URL will be checked against a known list of malicious sites. If the site is known to be malicious (i.e., the link could be asking you to provide login credentials), you will be notified by one of the following messages:

  - If known to be malicious by ATP, the message will read "This website has been classified as malicious."

  - If known to be malicious by TTU, the message will read "This website has been blocked per your organization's URL policy."

Otherwise, you will continue to the original site. This scan is almost instantaneous, and you may not notice.

- ATP will also scan all email attachments and remove those that are determined to be malicious. Messages containing large attachments may be delayed slightly, typically less than one minute.

As a reminder, the TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU information resources and data:

- Do not click on links contained within an email or SMS, unless you are certain of the sender's identity and expecting the information;

- Do not open attachments unless you are certain of the sender's identity and expecting the information;

- Delete and do not reply to any suspicious or suspect emails;

- Update your desktop, laptop, and/or mobile device anti-virus software; and

- Keep current on critical system updates:
  Windows: https://www.askit.ttu.edu/windowsupdate
  macOS: https://www.askit.ttu.edu/macupdate
  iOS: https://www.askit.ttu.edu/iosupdate
  Android: https://www.askit.ttu.edu/androidupdate

In addition, if you have confirmed or believe your information is compromised, the following options are available:

- Enroll with a credit monitoring service;

- Enable account alerts for important accounts, e.g., credit card accounts;

- Monitor your bank and credit card statements closely for suspicious activity;

- If you find evidence that your identity has been stolen, report it immediately to identitytheft.gov;

- Consider registering for fraud alerts with all credit bureaus (Equifax, Innovis, Experian, and TransUnion);

- Alternatively, consider utilizing credit freezes with each of the credit bureaus. If you intend to apply for a loan or credit card, you must provide the PIN given to you during the credit freeze setup process. This service may require a small fee; and

- At least once a year, obtain and review your free annual credit reports from annualcreditreport.com.

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips online at cybersecurity.ttu.edu. For more information or if you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

TEXAS TECH UNIVERSITY
Information Technology Division

visit **cybersecurity.ttu.edu** for more information

Acceptable Use Policy

As you take advantage of the many information resources provided by Texas Tech University, please remember that use of these resources must adhere to TTU Operating Policies and Procedures, including the IT Acceptable Use Policy. Based on Texas Administrative Code (TAC), the Acceptable Use Policy defines your personal responsibilities when using TTU information resources. Examples of institutional information resources include, but are not limited to, mobile devices, electronic files, data, computer hardware and software, peripherals, networks, etc. Acceptable Use Policy highlights:

- The TTU policy applies to all TTU faculty, staff, students, and others granted access to any University information resources, regardless of location or method of access;
- Information resources must be used in a manner consistent with the mission and objectives of TTU and the State of Texas;
- TTU faculty, staff, and students must only use information resources they have been granted access to and no one may attempt to circumvent IT security measures;
- Information on safe computing practices is available for the campus community at cybersecurity.ttu.edu;
- Be respectful, courteous, and ethical in the use of information resources;
- Do not share information resources login information (e.g., eRaider password). Account owners are personally responsible for all uses associated with their account;
- Incidental personal use is restricted to authorized users within certain guidelines (outlined in the Acceptable Use Policy);
- TTU information resources must not be used for personal or commercial gain or for political activity; and
- All use of information resources is governed by local policies and applicable state and federal law.

We invite you to review the complete list of TTU IT Security Policies at infotech.ttu.edu/security. In all things at Texas Tech University, integrity matters!

Beware of Text Messages Claiming Financial Payments Are Due

The TTU IT Division has received information that scammers are actively targeting individuals, including parents of college-age students, through SMS text messages, fraudulently claiming to represent Texas Tech University Student Business Services. The text messages indicate that the TTU payment system is unavailable for payment processing, which is not the case. They then direct the recipient to send payments through an online payment service, such as Zelle, PayPal, or Venmo. The victim may also be asked to provide sensitive personal information, such as birth date, SSN, mother's maiden name, and payment information, such as card numbers, expiration dates, and 3-digit security codes. If you have received one of these scams, do not respond. To verify if a text message is legitimate, contact Student Business Services at (806)742-3272 or sbs@ttu.edu. Please note that TTU Student Business Services does not use text messages to send these types of communications to students or parents. Please share this information with your parents or guardians as appropriate.

The TTU Office of the CIO reminds all students, faculty, and staff to stay vigilant and protect yourself, TTU data, and institutional information resources.

Common tactics that scammers use:

- Scare tactics. These aggressive and sophisticated scams try to scare people into providing confidential information or money. Many phone scams use threats to try to intimidate you and may also leave "urgent" callback requests, sometimes through automated email lists or phone calls ("robo-calls");
- Requests for immediate action or information. These callers often request personal information such as birth date, SSN, mother's maiden name, etc. under the guise of "verifying the caller's identity." They may also ask for money, gift cards, credit card numbers, or money transfers such as Western Union;
- Caller ID spoofing. Scammers often alter caller ID to make it look like a particular organization or an official agency is calling. The callers may use official titles and fake premises to appear legitimate. They may use online resources to get your name, address, and other details about your life to make the call sound legitimate; and
- Phishing email and regular mail. Scammers copy and use official letterhead in email or regular mail they send to victims in an attempt to make the scam look official.

We encourage you to be vigilant in practicing cybersecurity and invite you to learn more cybersecurity tips online at http://www.cybersecurity.ttu.edu.

For more information, assistance, or if you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

IT Security and Network Connectivity

Although convenient, public wireless connections are typically not secure. Your home or personal Wi-Fi system may also present security risks. TTUnet Wi-Fi service on campus is secured using industry standard and proven security practices. However, most public Wi-Fi available in retail stores, hotels, airports, and conferences are configured for convenience rather than security.

- Public Wi-Fi precautions:
    - Avoid using public hot spots for important transactions, such as transactions that require a login. You should not make financial transactions or use credit cards over public Wi-Fi.
    - If you are logged into a website or a program, be sure to log out when you are finished.
- Home Wi-Fi precautions:
    - Change the default password when setting up your home Wi-Fi.
    - Enable your Wi-Fi router's strongest security features, such as WPA2.
    - Disable remote administration (a feature on newer Wi-Fi routers that allows administration of the router from the Internet).
    - Make sure your home Wi-Fi access is password protected because “drive-by hackers” or your neighbors could gain access to your wireless network, steal your personal information, or participate in illegal online activities that could trace back to you.
    - Be selective about providing home Wi-Fi access to guests.
    - Create and use strong, unique passwords for all accounts.
    - Install anti-malware/anti-virus software on your computers and devices; Symantec Endpoint Protection is free for home use – just download from https://eraider.ttu.edu.
- Update operating systems, anti-malware/anti-virus software, application software, and mobile apps:
    - Windows: www.askit.ttu.edu/windowsupdate
    - macOS: www.askit.ttu.edu/macupdate
    - Android: www.askit.ttu.edu/androidupdate
    - iOS: www.askit.ttu.edu/iosupdate
- Use screen locks and passcodes on your devices.
- Back-up your content.
- Additional Information:
    - IT Operating Policies: http://www.depts.ttu.edu/infotech/policies.php
    - IT Security Policies: http://www.depts.ttu.edu/infotech/security/
    - Cybersecurity Awareness Program: http://www.ttu.edu/cybersecurity/
    - TTU Software Download: www.eraider.ttu.edu
    - Symantec: www.askit.ttu.edu/symantec

Keeping Systems Updated

On October 13, 2020, Microsoft will end service and support for Office 2010 for Windows and Office 2016 for Mac. As of this date, Microsoft will discontinue patches and upgrades to these applications; Microsoft will no longer actively protect those platforms. As a result, any computer continuing to use this software will have increased exposure to security risks, exploits, malware, and viruses. Beginning October 13, IT security scans will flag these systems as no longer compliant with TTU Operating Policies.

Additionally, on this date, Office 2013 for Windows connectivity to Office 365 will no longer be supported by Microsoft. Users may experience performance, reliability, and increased security issues when using these clients after this date.

We strongly recommend that users of these older Microsoft Office products upgrade to Office 365. Please begin reviewing departmental and home computer systems. All systems must be updated prior to October 13, 2020, and we offer the following resources to assist you:

How to Upgrade to Office 365: https://askit.ttu.edu/o365apps

New Computer Purchases: https://www.depts.ttu.edu/ithelpcentral/recommend

If you have any questions or need assistance, please contact your department’s local IT support staff or IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu.