Information Technology Division Bulletin
vol. 16 no. 3 | October 2019

We Are All Responsible

Cybersecurity Awareness Month Special Edition

Acceptable Use Policy | Facebook Security | Protecting Personal and Institutional Data | Internet of Things (IoT) | Are You a Target? | Venmo Scam

Message from the CIO

The National Cyber Security Alliance designates October as "National Cybersecurity Awareness Month." For the past 15 years, Texas Tech University has participated, hosting a number of educational activities for faculty, staff, and students. As cybercrime continues to proliferate and cyber criminals become increasingly savvy, we must all be vigilant and practice safe computing. We encourage you to review the materials provided in this issue. Our goal is to raise cybersecurity awareness and protect TTU information resources and data. Many of these tips will also help you protect your personal devices and data. Remember to think before you click. . . **we are all responsible**. Go Tech!

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

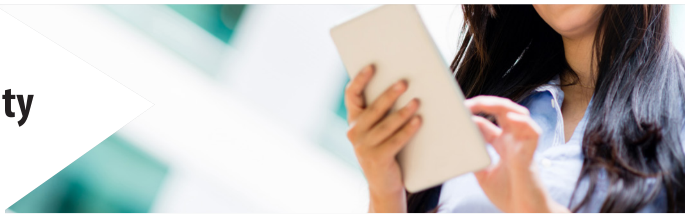
Acceptable Use Policy

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!

Facebook Security



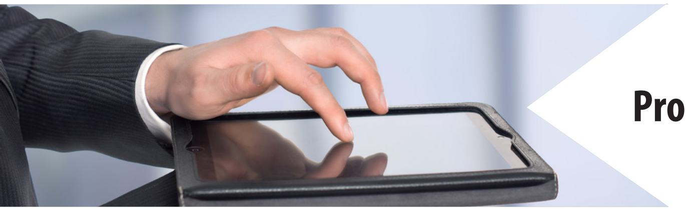
Facebook users may unknowingly be promoting malicious content due to an Internet scam called "like-farming." The act of Facebook "liking" may now have unintended consequences. Seemingly benign Facebook posts that appeal to one's emotions can potentially be ploys for scammers to accumulate "likes" and "shares" from these posts.

Once a post has gained enough popularity, the scammers modify the content, replacing the promotional content with malware, and infecting those that "like" and "share" the page. Common characteristics of "like-farming" attempts:

- Posts that promise to raffle off expensive gifts if it is "shared" and "liked;"
- Invitations that ask a user to "like" or "share" to show appreciation;
- Any solicitations that thrive on the good nature of people and play to their emotions; and
- Sites that appear on your news feed identifying people that have also "liked."

TTU IT recommends that you routinely review your activity log by clicking "Activity Log" located on the right-hand side of your cover photo when viewing your Facebook page, and select "Likes and Reactions" under "Filters" on the left-hand side of the screen. If any of the activities in your log look suspicious, you can delete, "unlike," and report the incident to Facebook.

Help spread "like awareness" and understand that not every Facebook page is an accurate representation of the true owner, and criminal motives are often well disguised. As you use social networking tools, we strongly recommend that you limit your "likes" and scrutinize your "shares." For more information on security and social media, please visit cybersecurity.ttu.edu.



Protecting Personal and Institutional Data

In the context of the massive Marriott (consumer.ftc.gov/blog/2018/12/marriott-data-breach) and Capital One (consumer.ftc.gov/blog/2019/07/capital-one-data-breach-time-check-your-credit-report) data breaches, 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, and selecting "Manage Your Account" and then selecting "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 the 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 Users:
  support.microsoft.com/en-us/help/12373/windows-update-faq
  - Mac Users:
  support.apple.com/en-us/HT201541
  - iOS Users:
  support.apple.com/en-us/HT204204
  - Android Users:
  support.google.com/android/answer/7680439?hl=en

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 questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

OCTOBER IS CYBERSECURITY AWARENESS MONTH
You know your identity, but who else does?

TEXAS TECH UNIVERSITY
Information Technology Division

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

Internet of Things (IoT): "Smart" May Not Be Safe

Doorbell...
Garage door...
Thermostat...
Refrigerator...
Automobile...
Washer and dryer...
Home entertainment system...
Baby monitor...
Home security system...
Smart home assistance...
...How many of these devices do you have?

Internet innovation has transformed the way we conduct commerce, secure our homes, manage our daily lives, and access entertainment. While the advancements have likely improved the quality of life for many, the convenience should be weighed against the risk to your personal information and safety. Our strategic TTU partner, Symantec, published a compelling article to help consumers secure IoT devices. The following recommendations are adapted from a recent Symantec Security Center article (full citation at the end of the article):

1. Give your device a name.
All devices are assigned a default name by the manufacturer—it might identify the make or model. Rename the device something unique and not identifiable to your location and identity.

2. Use a strong encryption method for Wi-Fi.
When you establish your home wireless network, select a strong encryption method like WPA2, to protect your network and communications.

3. Set up a guest network.
Keep your Wi-Fi account private. Visitors, friends, and relatives can log into a separate network that does not tie into your IoT devices.

4. Change default usernames and passwords.
Cybercriminals probably already know the default passwords that come with many IoT products. That makes it easy for them to access your IoT devices and, potentially, the information on them.

5. Use strong, unique passwords for Wi-Fi networks and device accounts.
Avoid common words or passwords that are easy to guess, such as "password" or "123456." Instead, use unique, complex passwords made up of letters, numbers, and symbols, if possible.

6. Customize the settings for your devices.
Your IoT devices might come with default privacy and security settings. You might want to consider changing them, particularly those that allow the manufacturer to collect and transmit your information.

7. Disable unneeded features.
IoT devices come with a variety of services such as remote access, often enabled by default. If you don't need it, be sure to disable it.

8. Keep your software up to date.
When your smart phone manufacturer sends you a software update, do not put off installing it. It might be a patch for a security flaw. Mobile security is important, since you may connect other devices through your mobile device. Your IoT device manufacturers may also send updates to your devices — or you might have to visit their websites to check for them. Be sure to download updates and apply them to your device.

9. Periodically review your IoT devices.
It could be time to upgrade older devices. Routinely check for newer models that might offer stronger security.

10. Do the two-step.
Two-factor authentication (2-FA)—such as a one-time code sent to your cellphone—adds a layer of security that can thwart criminals. If your smart-device apps offer 2-FA, please consider using it to protect your information.

11. Avoid public Wi-Fi networks.
You might want to manage your IoT devices through your mobile device in a coffee shop across town. If you're on public Wi-Fi—generally not a good idea—use a VPN.

12. Watch out for outages.
Ensure that a hardware or power outage does not restore the default manufacturer settings, leaving your device in an unsecure state.

Copyright © 2019 Symantec Corporation. Symantec Security Center, 2019, "12 tips to help secure your smart home and IoT devices (Adapted from the following publication: https://us.norton.com/internetsecurity-iot-smart-home-security-core.html)

20.4 Billion

IoT Devices will exist by 2020

Gartner 2019

Are You a Target?

Your mother's maiden name...
Your first car...
Your pet's name...
Your place of birth...
Your favorite color...
Your High School mascot...
Your anniversary date...
Name of your first born...

Is any of that information about you posted on Facebook? Twitter? LinkedIn? Instagram? Any public website? Is any of this information used as a password to your banking accounts? Other financial accounts? eCommerce sites? PayPal? Internet criminals are getting more creative in mining personal data to aid in guessing password reset questions and passwords. If successful in resetting your password, then they can access your account and information. These exploits continue to grow because people use common information for reset questions and/or passwords, and criminals continue to profit from personal information theft.

We suggest the following safe computing practices:

- Review all the information you have published on websites and in social media, and remove anything that answers any of your password reset questions;
- Change any password reset questions that use information you had previously published publicly;
- Use different strong passwords for accounts, such as banking, credit, or investment accounts. You should not use your eRaider password for any accounts other than eRaider; and
- If you need to write down your passwords to remember them, write down a clue that will help you remember, but will be meaningless and undecipherable to others.

Working together, we can protect institutional and personal data, and make these strategies less lucrative for criminals. For information about improving your own personal cybersecurity, please visit cybersecurity.ttu.edu. For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Consumer Alert: Venmo Scam

Reprinted from Consumer Affairs, "Authorities Remind Consumers to be Aware of Venmo Scams." (Mark Huffman, 9-19-2019) consumeraffairs.com/news/authorities-remind-consumers-to-be-aware-of-venmo-scams-091919.html

If you use Venmo to make payments to friends and family members, there are scams you need to be aware of that attempt to exploit the platform and law enforcement officials recently reported a new one.

Scammers have been sending text messages to Venmo users, mimicking the app's appearance, telling them their accounts will soon be charged. If they don't recognize the payment, they are told, they should log into their accounts to dispute it.

The text reportedly allows users to easily access their accounts but asks for personal information to identify the user. If that information is provided it is stolen and then sold on the dark web.

Law enforcement officials warn Venmo users not to use any information provided in a text to enter their account. Instead, they are advised to use either the Venmo app or the webpage.

A year ago, Venmo parent company PayPal reached a settlement with the Federal Trade Commission (FTC) after the agency charged it with failing to protect users' privacy and misleading them about the money in their accounts.

The FTC claimed that Venmo did not adequately explain how money is transferred from a Venmo account to a bank account and did not employ proper security safeguards. The agency said it has been too easy for scammers to take advantage of these features and take users' money.

Scammers often target apps used to move money, and Venmo has been no exception. In one scam, the FTC says a seller might send off a purchased item after being informed that funds had been transferred to their Venmo account.

But in some cases, the agency says the scammer, posing as a buyer, could ask Venmo to reverse the charge and obtain the item without having to pay for it.

The FTC says there are ways to protect yourself. When using an online platform to buy or sell, check to see what kind of insurance policy it offers. Some platforms have excellent coverage, waiving charges if there is a problem.

Authorities say consumers using an online platform to buy or sell should exercise caution, especially when dealing with a stranger. If something doesn't seem quite right, they say, don't go through with the transaction.