From Here, It’s Possible

Records Retention Tips from TTU University Archivist Lynn Whitfield

...every 3 seconds

an identity is STOLEN!

What are YOU doing to protect yourself?

October is Cyber Security Awareness Month.
Visit SafeComputing.ttu.edu for tips to protect yourself online

Stop. Think. Connect.
National Cyber Security Awareness Month
staysafeonline.org - stopthinkconnect.org - onguardonline.gov

1...2...every 3 seconds
an identity is STOLEN!

What are YOU doing to protect yourself?

October is Cyber Security Awareness Month.
Visit SafeComputing.ttu.edu for tips to protect yourself online

Stop. Think. Connect.
National Cyber Security Awareness Month
staysafeonline.org - stopthinkconnect.org - onguardonline.gov
The Lowest Wave: Phishing Attempts on Mobile Devices

Cyber criminals are constantly adjusting their attack strategies based on changing consumer behaviors. One such example is phishing attempts targeted at those who check their email using their mobile devices. Cyber criminals exploit our growing use of mobile devices in order to steal confidential/sensitive information and contact/friends lists.

The TTU IT Division offers these tips to protect you from falling victim to phishing attempts on your phone:

- When reading email or checking your social networking sites such as Facebook, Twitter, and LinkedIn, carefully scrutinize email and links posted to a wall or news feed. Do not click on a link unless you are sure it is legitimate.
- Check the URL in your mobile browser to ensure it is a legitimate website. Any website that asks for your login/account information should display a lock in the address bar of your browser or “https://” in front of the web address.
- If possible, avoid conducting financial transactions and other sensitive business on your mobile device—only use apps and links provided by your bank.

Best Practices for Using Removable Media

The popularity of removable media has grown at an impressive rate as users are drawn to the convenience of storing and transporting data quickly for use on multiple systems. As is the case with many technological advances, some of the characteristics that make removable media convenient also introduce security risks.

Removable media devices come in various forms that include, but are not limited to: USB drives, flash drives or cards, read/write optical discs (CD and DVD), memory cards, external hard drives, Personal Digital Assistants (PDA), and personal media players. Attackers masquerade as legitimate media to infect systems with malicious code and/or to remove sensitive data, such as usernames, passwords, and encryption keys from user systems. Additionally, removable media, such as USB drives, can be easily lost or stolen, and could result in criminals obtaining sensitive business data.

The TTU IT Division and CERT (United States Computer Criminals obtaining sensitive information. The TTU IT Security policies at www.depts.ttu.edu/infotech/security, specifically, the policies on Acceptable Use, Information/Data Classification, and Privatelitely address individuals’ responsibility to safeguard confidential data.

For assistance in managing or configuring your removable media, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu, or online at www.ithelpcentral.ttu.edu.

Protecting Institutional Information Resources

As employees of a state institution and in the course of our work duties, we all have a responsibility to protect institutional information resources and data, especially confidential information, such as social security numbers, student grades, home addresses, financial information, etc. The TTU IT Security team recommends that you familiarize yourself with the following TTU Operating Policies (www.depts.ttu.edu/infotech/ops/):

52.01 - Information Technology Operations
52.02 - Infringement of Copyrights in Information Technology
52.03 - Obtaining Data Network Services
52.04 - Information Technology Security
52.05 - Electronic and Information Resources Accessibility
52.06 - Project Management Practices
52.07 - Website Operations
52.08 - Payment Card Information Processing By University Departments
62.14 - Red Flag Rules
30.22 - Guidelines For The Educational Use Of Copyrighted Works
48.04 - Cellular Telephone Policy

Don’t be “Tricked” by Scareware

Internet criminals are becoming more cunning and creative in their tactics to steal your identity. Being knowledgeable about the threat of scareware can help you avoid becoming a victim. Scareware is a tactic used by Internet criminals to lure you into downloading and purchasing fake antivirus software, by convincing you that your computer is infected with a virus. The “updater” or “alerts” in these programs will call for you to take some sort of immediate action, such as clicking to install new software, accepting recommended updates, or removing unwanted viruses or spyware. Once you click on an option, the rogue software downloads to your computer.

The TTU IT Division recommends the following safe computing tips to help protect yourself from this and other online scams:

- Do not install unfamiliar antivirus/anti-Spyware software;
- Do not give your credit card information to an online vendor, unless you are certain that they are legitimate and the transaction is secure. Most secure website addresses will begin with “https://” or your browser will display a padlock at the bottom of your browser window;
- Use automatic updating features to keep your operating system and virus protection software updated;
- If a website appears suspicious, investigate its legitimacy and learn more before providing any information. It’s better to be safe than sorry!

Additional Safe Computing information can be found online at safecomputing.ttu.edu.

Break the Chain – Understanding the Dangers of Forwarding Email Chain Letters

A chain letter is any email message that implicitly or explicitly encourages the recipient to forward it to others. Chain letters are not only a potential annoyance, but can be a ploy to spread a malicious virus or to remove personal information.

To forward the threat of scareware can help you avoid becoming a victim. Scareware is a tactic used by Internet criminals to lure you into downloading and purchasing fake antivirus software, by convincing you that your computer is infected with a virus. The “updater” or “alerts” in these programs will call for you to take some sort of immediate action, such as clicking to install new software, accepting recommended updates, or removing unwanted viruses or spyware. Once you click on an option, the rogue software downloads to your computer.

In addition to the threat to TTU data and IT resources, chain letters are easily copied in other ways:

- use network/internet bandwidth;
- consume storage space on mail servers and desktops;
- may allow valuable faculty and staff time and;
- may offend and/or annoy the recipient.

Please do your part to ensure the safety and security of TTU information resources and do not forward chain letters.

Best Practices for System and Lab Administrators

- Administrators must assess the risk of using removable media devices for business needs in their area.
- If possible, restrict using personal removable media devices with TTU-owned systems and vice versa.
- Lock USB ports and control the use of USB ports using configuration control software.
- Block unauthorized peripheral devices from being used in a system.
- Disable “auto run” and “auto play” features at the operating system level.
- Consider limiting the number of workstations that allow the use of removable media devices.
- Ensure the use of removable media is auditable.

For assistance in managing or configuring your removable media, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu, or online at www.ithelpcentral.ttu.edu.

Protecting Institutional Information Resources

As employees of a state institution and in the course of our work duties, we all have a responsibility to protect institutional information resources and data, especially confidential information, such as social security numbers, student grades, home addresses, financial information, etc. The TTU IT Security team recommends that you familiarize yourself with the following TTU Operating Policies (www.depts.ttu.edu/infotech/ops/):

52.01 - Information Technology Operations
52.02 - Infringement of Copyrights in Information Technology
52.03 - Obtaining Data Network Services
52.04 - Information Technology Security
52.05 - Electronic and Information Resources Accessibility
52.06 - Project Management Practices
52.07 - Website Operations
52.08 - Payment Card Information Processing By University Departments
62.14 - Red Flag Rules
30.22 - Guidelines For The Educational Use Of Copyrighted Works
48.04 - Cellular Telephone Policy

Don’t be “Tricked” by Scareware

Internet criminals are becoming more cunning and creative in their tactics to steal your identity. Being knowledgeable about the threat of scareware can help you avoid becoming a victim. Scareware is a tactic used by Internet criminals to lure you into downloading and purchasing fake antivirus software, by convincing you that your computer is infected with a virus. The “updater” or “alerts” in these programs will call for you to take some sort of immediate action, such as clicking to install new software, accepting recommended updates, or removing unwanted viruses or spyware. Once you click on an option, the rogue software downloads to your computer.

The TTU IT Division recommends the following safe computing tips to help protect yourself from this and other online scams:

- Do not install unfamiliar antivirus/anti-Spyware software;
- Do not give your credit card information to an online vendor, unless you are certain that they are legitimate and the transaction is secure. Most secure website addresses will begin with “https://” or your browser will display a padlock at the bottom of your browser window;
- Use automatic updating features to keep your operating system and virus protection software updated;
- If a website appears suspicious, investigate its legitimacy and learn more before providing any information. It’s better to be safe than sorry!

Additional Safe Computing information can be found online at safecomputing.ttu.edu.

TEST YOUR IT IQ

True or False: Using your pet’s name spelled backwards is a safe password.

Passport Tips

Avoid using information about you as passwords, such as:
- Your name, nicknames, username or family members’ names - including pets;
- Your birth date, credit card number, or driver’s license number;
- Your Social Security Number;
- Your address, phone number, license plate, or town/city/state;
- Your hobby, favorite color, or other personal preferences;
- Words found in a standard dictionary;
- School mascots or slogans;
- Popular acronyms or slang; and
- Reverse spelling of any of the above; sophisticated programs can easily reverse the spelling.

Ideas for creating a strong password that is easy to remember:
- Create your own combination of information and change portions of the pattern every ninety (90) days;
- Select a phrase and substitute numbers or special characters for the letters;
- Combine parts of an important date with a name, address, location, or event; or
- Start with a date and subtract a number from it, then add initials that you will remember.