another and help us all be more secure in our cyber world by giving us multi layers of protection. Adhering to this checklist won't ensure perfect security, as nothing can. However, it certainly can help us become a smaller target and reduce the attack surface for the cybercriminals.

If we plan properly and prepare for our digital life as we do (or should do) in our real life, we will be in a better position to enjoy the benefits resulting from technology changes rather than being constantly stressed by the threats from cybercriminals. Let's enjoy life along the way. As John Lennon sang in "Beautiful Boy", "Before you cross the street take my hand. Life is what happens to you while you're busy making other plans."

Texas Tech University Public Cybersecurity Site
www.cybersecurity.ttu.edu

National Cyber Security Alliance
www.staysafeonline.org

StopThinkConnect
www.stopthinkconnect.org

Federal Trade Commission
www.consumer.ftc.gov/features/feature-0038-onguardonline
www.consumer.ftc.gov/features/feature-0014-identity-theft

Free Credit Report
www.annualcreditreport.com

Credit Reporting Agencies
Equifax - www.equifax.com
Experian - www.experian.com
TransUnion - www.transunion.com

Scam Lists
www.scambusters.org
www.fbi.gov/scams-and-safety
www.consumer.ftc.gov/scam-alerts
www.usa.gov/stop-scams-frauds

FBI Internet Crime Complaint Center
www.ic3.gov/media/default.aspx

National Do Not Call Registry
www.donotcall.gov

Mail | Mail Stop 2008
Phone | 742-5151
Fax | 742-5155

TTU IT

View IT Bulletins online at
infotech.ttu.edu/itbulletin

Need IT assistance?
IT Help Central
(806) 742-4357 (HELP)
ithelpcentral@ttu.edu

Computer-Based Training (CBT):
www.cbt.ttu.edu

Information Technology Division Bulletin
Special Edition
vol. 14 no. 2 | September 2017

Message from the CIO

As requested by several campus administrators and individuals, we are providing an article that I wrote for **Education Technology Insights** earlier this year. Protecting individual and institutional data and information resources continues to be a challenging endeavor in the workplace, as well as at home. We hope you find these **survival tips** to be useful in protecting all the confidential and sensitive information in your life and at work. Especially because of the recent growing number of aggressive phishing attempts that we have seen at TTU, please take a moment to review these tips and share them with others in your area or life. When it comes to the protection of institutional and personal data, we are all responsible!

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

Running the Gauntlet in Your Digital Life: Top 25 Survival Tips

Sam Segran, (June 2017), Education Technology Insights (Unabridged Version)

Over the last twenty years, I have been providing volunteer cybersecurity and cybersecurity awareness lectures to children of all ages, K-12 students, business communities, computer science and information systems classes, university faculty/students/staff, and to retirees (generally the people with the most assets to protect and the least knowledge to protect themselves online.) At the end of most of these sessions, I left the audience with a quick cybersecurity checklist. In the early years, it was just a few items. Since then, my list has steadily grown to 25 items as our digital world has expanded.

While this checklist is intended as a personal checklist, there are many items in the list that are still applicable to organizations as well. The checklist may be obvious to many in the IT field. However, in my experience, no one is really fully protected from some of the modern day cybercriminals; especially from cybercriminals who are skilled and have access to hacker tools and their own tech support from underground, cybercriminal organizations.

1. Personal Responsibility—We all have a personal responsibility to protect ourselves and our loved ones. Complacency by individuals, especially in organizations, is usually a common element in data compromises. There is a common misconception among some individuals that "the IT security people and the firewalls will protect me." These individuals need to realize that unless stringent security controls are enforced, a careless click on a mal-link may still lead to a compromise. Even worse is when individuals willingly surf to a website and divulge their credentials in anticipation of some goods or rewards. Hackers are also getting smarter, diminishing the obvious errors and typos in phishing emails. Spear phishing attempts are more strategically planned and crafted, complete with authentic looking logos, and correct names and titles of officers in the organizations.

2. Data Clutter and Spring Cleaning—Reduce that data clutter. Don't become a data hoarder! Minimize your stored information, especially confidential or sensitive information. Over time, people forget how much confidential or sensitive data they have accumulated, sometimes even other people's confidential or sensitive data. Establish a Spring Cleaning (or Christmas Cleaning) routine. At least once a year, review your digital life and secure it. Delete older and/or unneeded digital files and clear that clutter. Review your account set-ups. Review your backups.

3. Updates—Where possible, enable automatic updates of operating systems, applications, anti-virus software, and apps. While more secure systems are emerging such as cloud-based tablets, notebooks, and operating systems as a service, the currently installed base of consumer and business devices still require updates as vulnerabilities and exploits are identified. For business devices, a managed approach is advisable.

4. Anti-Virus Software—Use it and keep it updated.

5. Screen Locks—Deploy screen locks for computers, tablets, and smartphones. Whether a simple 4-digit PIN or a more complex method, this is the simplest and first line of defense for most systems.

6. Passwords—Use strong passwords. Unfortunately, not all service providers use best practices for password acceptance by their systems. Hackers can get access to online dictionaries in multiple languages and to rainbow tables, pre-computed tables of information for reversing cryptographic hash functions, usually for cracking passwords. Where possible, use longer passwords, or

password phrases rather than simple words that may be found in a dictionary. Do not re-use old passwords. Use different passwords for different services, especially if these services are important, such as primary email accounts, bank accounts, investment accounts, etc. Create a system that is unique to you. With the many different online services that an individual has, it may help to inventory and update these during the annual Spring Cleaning routine. If you must write them down, write down clues rather than the passwords. Keep them in a secure location such as a safe or a bank vault deposit box. Treat them as carefully as your important documents. If you wish to use a password manager, consider carefully when and where to use it based on your comfort level. An option may be to use a password manager to manage most of your accounts, and keep your most confidential and/or sensitive account passwords separate.

7. Password Recovery—Thankfully, password recovery methods are no longer just password recovery questions for major service providers. The dated, standard password recovery questions are easily used by hackers to breach accounts. The limited set of questions where responses may be guessed or easily found on social media, combined with people's honesty in answering these questions, make this an easy way for hackers to breach an account. This is possibly the one time in your life, it is OK to intentionally give an erroneous response if you are forced to use this method. However, don't forget your responses!

8. Multi-Factor Authentication—Wherever possible, use multi-factor authentication, especially for important accounts and services. At the basic security level, an individual has three types of credentials (factors), what you know (e.g. username and password), what you have (e.g. smartphone or physical token or smartcard), and what you are (e.g. fingerprint or iris scan). Combining these different factors raises the confidence level that the correct individual is accessing the account. For the layman, as a general principle, it is safer to use a smartphone to recover your email account password than a second email. A hacker could have compromised both of your email accounts, especially if you are using the same password for the two email accounts or if your computer/device is already compromised without your knowledge.

9. Home Computer Accounts—As much as possible, instead of using the default Admin (privileged) account on home computers, set up a second Standard (non-privileged) account and use it for most of your activities, especially when browsing the web. Set up an additional Guest account if you have regular visitors or children who are allowed to use your home computer.

10. Hyperlinked Words or Links—Don't click on hyperlinks in other contents, e.g. in SMS, emails, websites, etc. Where possible, log into your actual accounts (FB, LinkedIn, etc.) or open a browser and type in the URL. If that is not possible, mouse over the link to ensure that it is the link that it purports to be. Especially beware of short URLs and QR codes when you can't see the full link to the website before you click.

11. Phishing Schemes—Think. Be wise. Be vigilant. Don't be fooled. Don't become a victim. Do not divulge personal credentials. No, it is not "THE IT Help Desk" asking for your credentials or helpful "Microsoft Tech Support" trying to fix your computer! Nor is it the IRS demanding your personal credentials via social media or email. And remember that scammers do change their tactics frequently to increase their payoffs.

12. Backup—Backup your data judiciously. Use automated backups. There are several, credible cloud-based automated backup solutions that are easy to use and reasonably priced. For the really important information, keep a separate, off-site backup that is refreshed periodically. This practice will be very helpful if you become a ransomware victim.

13. Account Profiles—Keep your account profiles updated, especially for primary emails, credit cards, bank accounts, investments accounts, retirement accounts, and other important accounts. Use the security features of your online accounts, e.g. set up multi-factor authentication. Another item to add to your Spring Cleaning routine.

14. Credit Card Alert Notifications—Enable alerts such as transactions above a set amount or even below a certain amount (sometimes cybercriminals test your cards with low purchase amounts that are then backed out and won't be reflected in your monthly statements.) Set up geographic alerts, e.g. purchases conducted in another country. Set up travel notices and alerts if you plan to travel overseas.

15. Credit Monitoring Services—While you may be able to do everything yourself that a credit monitoring service will do for you, it is certainly an option for most people, especially people who do not have the knowledge, time, or discipline to carry out all the tasks needed.

16. Credit Reports—Check your credit reports at least a few times a year. Verify that no one else has opened an account under your name.

17. Social Networks—Limit personal information (yours or others) exposed via your social media postings and/or profiles on social networks. Cybercriminals scan social media postings and social network profiles for useful information that can be used to compromise accounts, identities, or your (or your loved ones') personal safety. Spend some time learning about social networks and social media. They are here to stay. This is especially important if you have children who you need to protect from predators such as child molesters, stalkers, or bullies. Also be aware that in social networks, generally your "friends" aren't really your friends who have your wellbeing at heart.

18. Public Wi-Fi—Limit the use of public Wi-Fi. If feasible, just don't use it. Absolutely, do not use it to transmit sensitive information such as account usernames and passwords. If you know your data traffic is encrypted with a good standard, you may be alright, maybe... The risk in connecting through a public Wi-Fi is also the unintended consequence. Most mobile devices have dozens of apps that are constantly signed-in with the credentials stored on the device. The moment your device connects to a public Wi-Fi access point, many of these apps will rapidly transmit the stored credentials, faster than you can disable them, and some without your knowledge. Credentials that are not encrypted can be easily captured by a cybercriminal monitoring or controlling the Wi-Fi access point.

19. Bluetooth—People are increasingly using Bluetooth to connect their mobile devices to their vehicles, fitness trackers, earphones, watches, keyboards, etc. Similar to Wi-Fi, Bluetooth uses radio waves that can be easily captured by devices. Hackers can download your contacts, calendars, pictures, or other information from your phone, also known as "bluesnarfing". Some malware (like certain flashlight apps) can even spread to nearby devices that are discoverable via Bluetooth. There are four levels of Bluetooth security. Level 1 is the most vulnerable and are generally found in older devices. Security gets better at each level but is not foolproof. If possible, make your device non-discoverable. If feasible, turn Bluetooth off (when not using it or maybe when you're traveling). Do not lose control of your device, even temporarily, because hackers can establish a Bluetooth device connection quickly if they have physical control of your device.

20. Home Wi-Fi—Secure your home Wi-Fi network. Just because it says, "secure" on the box of your new access point, it doesn't necessarily mean it is secured by default. At a minimum, change the default admin password and turn on encryption (WPA2 recommended) when setting up your home Wi-Fi access point. While not perfect security, it will significantly improve it. Additionally, you could change the broadcast name (SSID) or not broadcast it, use MAC authentication, and/or disable the remote administration feature (if available).

21. Visual Hacking—Do not underestimate the damage that can be done with visual hacking, also known as shoulder surfing. Many people get so transfixed on their mobile devices that they become oblivious to their surroundings. A cybercriminal (or maybe someone who is close to you) can watch, and even record your keystrokes or screen swipes from a distance. Later they can use your credentials to compromise your accounts, or steal your device and use the stolen credentials to get through the screen lock.

22. Phone Calls—Don't underestimate the unsolicited phone call. Beware of phone scams that could eventually lead to account or data compromise. Hackers have become very good at using social engineering techniques to trick people into divulging confidential and/or sensitive information. Take advantage of the National Do Not Call Registry. It won't stop the nuisance telemarketing calls but may help reduce it, eventually.

23. Internet of Things (IoT)—One of the fastest growing threats to personal data security and safety is the explosion of the Internet of Things (IoT). IoT devices are generally daily-use appliances and other objects connected to the Internet that transmit and receive data. These devices include baby monitors, security cameras and systems, home alarms, building control systems, home appliances, medical devices, fitness devices, drones, automobiles, and many more. These devices are flooding the market at such a rapid pace for economic reasons that many of them are not properly secured and are easily compromised by hackers. Imagine a stranger watching your baby, listening in your bedroom, monitoring your activities at home, and even unlocking your doors from halfway across the world. It's chilling to just think of the possibilities that can result from IoT vulnerabilities. Some of the recent Internet slowdowns and website takedowns were committed by hackers who had gained control of thousands of IoT devices, including internet-connected cameras. Be aware of these pitfalls, learn the capabilities and vulnerabilities of the devices (e.g. from the manufacturer and published security articles), take the recommended steps (e.g. turning on encryption or setting/changing a password) to limit their vulnerability before accepting the risks and deploying them.

24. Death—Our digital world as most of us know it is a relatively young world—only about 20 years old. Eventually we will die. So, let's plan for it. As digital citizens and digital natives expire, we need to consider what happens to our data, accounts, passwords, online profile, etc. What you do with your digital life, including accounts, is your prerogative. Most major online providers have an established way to handle this issue, some better than others, generally in favor of individual privacy. To prevent identity theft or fraud, sometimes only the contents may be provided, after a proprietary vetting process, instead of full account access. Generally, the Terms of Service (TOS) of the service provider will address this issue. If no guidance is available from an online provider, you need to decide. One approach is to store important information in a location and tie that information specifically in your will (appoint a digital executor) or by using online methods if available, and let the others expire with you. There are also service providers that are emerging to meet this need. As always, get good legal advice in these instances before you decide.

25. Seek Help—Finally, seek help when you need it. If you have to pay for professional services, consider the cost of not doing it and becoming a cybercrime victim. Help is available in various ways, from cyber-savvy family members or friends, professionals, reputable forums, universities, non-profits, government, and other reputable online sources. A list of free resources is provided below.

Of course, each of the above items by itself will not secure someone's digital assets or life. In articles, conferences, and training, it is painfully disappointing to hear vendors and even IT security professionals disparaging one of these items in favor of another, e.g. knocking cybersecurity awareness in favor of security controls, or proclaiming anti-virus is dead because of advanced Artificial Intelligence-based advanced threat protections. These items should complement one