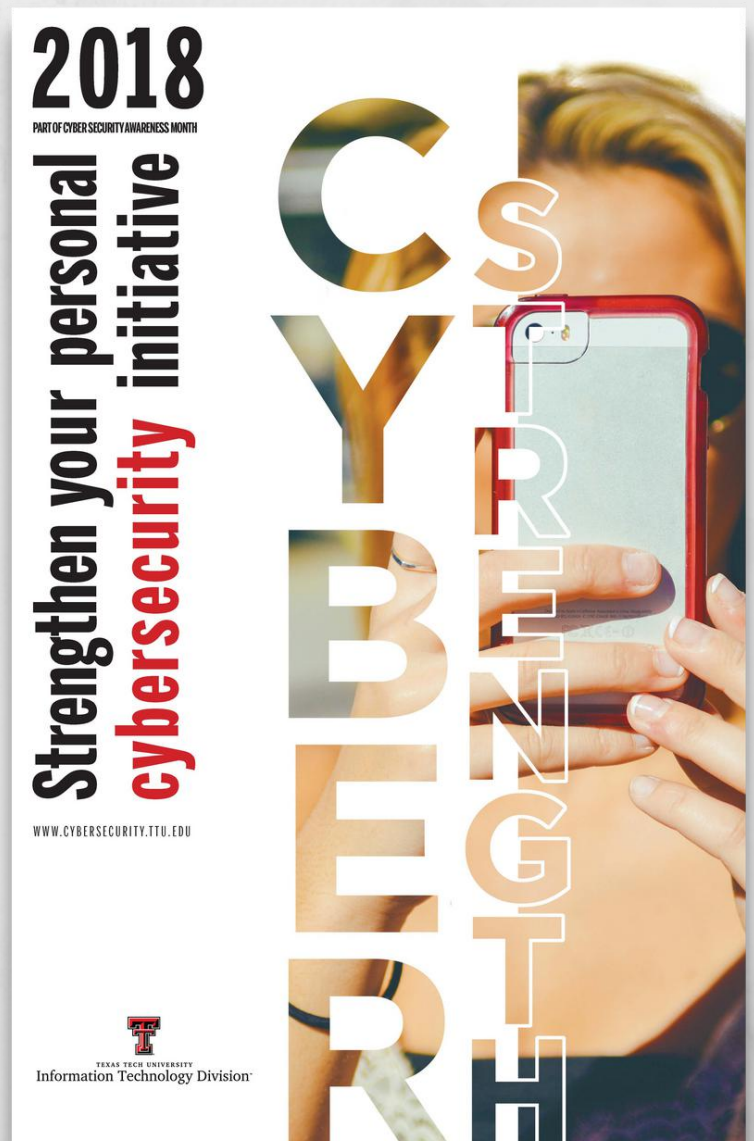
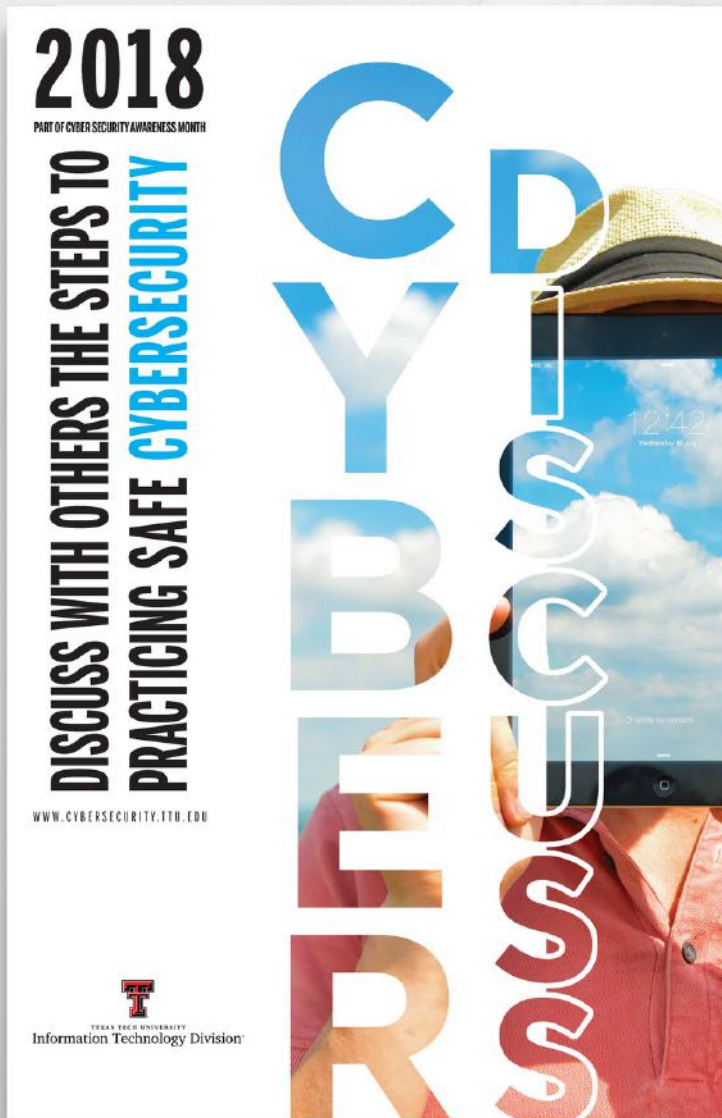


INTERNSHIP

Wanna see a magic trick? Type / on your keyboard...

Cyber Month

For this project we were given the task of creating posters for the Cyber Awareness Month in October. What I decided to do was incorporate text and photos together to bring a new and fun way of demonstrating the point across it was one of my most clean and favorite works I've done for the internship.



WIFI

Although convenient, public wireless connections are inherently less secure. You should avoid using public Wi-Fi for important transactions, such as transactions that require a login. You should also make financial transactions or use credit cards over public Wi-Fi. Checking your email or social media sites on public wireless connections could expose your information to hackers. You also run the risk of logging in, leaving your account open for the next person who uses the system. If you are also using a computer provided by the entity, your laptop or personal Wi-Fi system also presents security risks. Always change the default password when setting up your laptop Wi-Fi. Without a strong password, anyone who has access to your network could gain access to your wireless network and can read your personal information or participate in illegal online activities that will send you to jail. You should be careful with whom you share your personal Wi-Fi password. You should only share it with trusted users.

PHISHING SCAMS

Internet criminals and hackers often prey on their victims as a legitimate, trustworthy source to gain your trust when sending fraudulent messages. If you have any suspicion that a message is fraudulent or a scam, look out the sender or organization directly without using email. Reporting how to recognize a phishing scam can help you avoid "taking the bait" and becoming a victim.

Clues to help you spot a phishing scam

- Requests for your personal and/or financial info, including information and organizations you are required to provide information to.
- Too many requests for your account will be closed if you do not respond immediately or that your credit rating may be lost.
- No clear contact information in the "from" field or email signature.
- "Do not contact multiple numbers, email addresses or IP addresses."
- Unusual or unusual greetings, such as "Dear account holder."
- Unreasonable deadlines.
- Links that don't take you to the website or organization.
- Emails that address that you don't have, such as "John" or "Taylor," or links that you don't have accounts with.
- Emails that "test" addresses.
- Emails that sound like they are coming from a friend, but you don't recognize the name. They often ask you to confirm a friend request or attempt to establish a contact with a subject line such as "How are you?"
- Also you may see "mailto:" or "mailto:" in the subject line.
- Use common sense and do not click on links or download files from suspicious sources.
- Do not click on links to create accounts, log in, or verify identity or location.

MALWARE

Malware, short for "malicious software," refers to software designed to gather sensitive information, monitor your keyboarding or keyboard activity, gain access to a private system, or cause damage or disrupt a computer, server or network. Malware can be spread through emails, websites, and even apps. To protect yourself, update malware, firewall, and other anti-malware software on all your systems and devices. Also, configure your systems to automatically install updates and security patches. Awareness and knowledge of malware tactics will help you prevent your systems from becoming infected.

MOBILE DEVICES

If you always are carrying a mobile device, you should consider if you need "digital hygiene" or a strategy to protect it. Apps, the most significant security threats, are the most common cause of mobile device security breaches.

Best practices to help protect your mobile devices

- Use mobile device security features such as a password or biometric recognition.
- Maintain up-to-date software, including operating system and apps.
- Install anti-virus software, if available.
- Encrypt personal and sensitive data, when possible.
- Disable location and connectivity, such as Bluetooth or Wi-Fi.
- Set a screen lock and device to "wipe remotely," so that unauthorized devices cannot access data.
- Use caution when opening attachments or clicking links contained in text messages or email.
- Avoid posting sensitive Wi-Fi or mobile.
- Don't install apps you don't need and don't install apps.
- Delete all information stored by a device prior to the selling it, and
- Do not loan your mobile device to someone.

APPS

If you own a smartphone or a tablet, you may have downloaded apps for browsing or simple online banking, playing games, or connecting to social media networks. Cyber criminals are exploiting the rising demand for mobile apps by creating apps that contain malware.

Reputable app stores, like the Apple App Store, Google Play and Amazon, carefully evaluate apps and require that any app available in their store uses high security requirements before being released to consumers. Because of this, apps from these stores are usually much safer than apps, since they are less likely to require stringent code standards and formal app reviews.

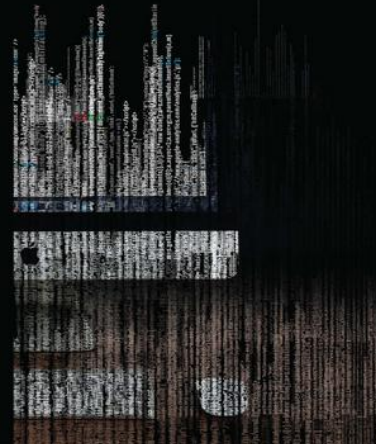
You should always use app operators when they are available. Apps operators add the latest features and apply security patches. Only install updates that create an update from the app store where you originally purchased or obtained the app. Don't install apps you don't need and delete unused apps.

ONLINE SHOPPING

Online shopping is convenient, but you have to be aware of the security risks involved. When completing your purchase, look for the lock icon on the browser's status bar and make sure that "https" appears in the address bar (http://...). Print and save records of your online transactions, especially online receipts and any electronic correspondence you have with the retailer or seller. Review your credit card and bank statements as you receive them and immediately report unauthorized charges. Use a cross-cut shredder to shred all documents when no longer needed.

CYBER SECURITY PRACTICES FOR TODAY'S DIGITAL CITIZEN

Cyber security is the practice of protecting our personal safety online, as well as keeping our personal information secure. Common sense, accountability, and responsibility are the cornerstones of cyber security. It is everyone's responsibility to practice and promote cyber security. Our goal is to empower you with the knowledge and tools to defend against Internet-based security threats.



TEXAS TECH UNIVERSITY
Information Technology
Division

— SPRING 2019 —

IDENTITY THEFT

Identity theft is the use of another person's name, identity, or other identifying information, without their consent, to obtain credit, services, or other benefits. Identity theft can occur in many ways, including through phishing, malware, and other means. Identity theft can be prevented by taking steps to protect your personal information.

Identity thieves use a variety of methods to steal your identity such as:

- Phishing by sending you text or email containing ID, social media cards and banking information.
- Tapping into your data through phishing and email scans, phone phish calls, or fake websites.
- Scanning social media accounts for personal details or clues to passwords and personal recovery questions.
- Scrolling through your trash looking for bills or other papers containing your personal information, commonly called dumpster diving, and
- Installing malware on your device without your consent or knowledge.

Protect your identity by using the following basic tips:

- Install anti-virus and other anti-malware software on all your systems and devices. Configure your system to automatically install updates and security patches.
- Never respond to email requests for account, password, or any specific account information or other sensitive information. Credit, insurance and organizations will not request personal information via email.
- Do not click on links in an email message, instant message, or social media posts unless you trust the sender and are expecting the information. If you are unsure, check with the sender directly before clicking on links.
- Use a cross-cut shredder to destroy documents containing personal information.
- Shop only at reputable and secure Internet locations. Make a point to look for the "https://" in the address bar, and
- Regularly review your credit card bills carefully and have alerting any change that you do not recognize.

PASSWORDS

Use passwords on the electronic systems to which you have access. Developing strong passwords will help your personal information and identity more secure.

Suggestions for creating strong passwords

- Consider starting with a sentence or phrase that is meaningful to you, but not a common sentence or phrase.
- Remove the spaces between the words in the sentence.
- Convert the words into "shortened" and/or intentionally misspell a word, e.g. HM for home.
- Add length with numbers and symbols that are meaningful to you, and
- Use at least eight characters with a mix of upper and lower case numbers, letters, and special characters (e.g., @, #, %).

Additional best practices for passwords

- Create unique and complex passwords for each of your accounts. If an identity thief obtains one of your passwords, they will likely try to use multiple accounts.
- Avoid using personal information such as birthdays, pet names, favorite color, initials, or birth date as shared across passwords or personal recovery questions. This information could easily be discovered on social media sites. Consider using false answers to password recovery questions that only you would know.
- Avoid using words found in the dictionary, popular slang, or acronyms when creating passwords.
- Change your passwords on a regular basis for change every 90 days.
- Consider using a password manager to help you create and store all your passwords. Therefore, you only have to remember the password to the password manager.
- Use multi-factor security features such as a password or biometric recognition.

SOCIAL NETWORKING

When you share and post online, it is critical that you think before you post, tag, retweet, comment, forward, or send. Once photos, videos, or content is shared in the digital world, it is almost impossible to delete. "HTTPS" - would take you - means that the website you are visiting is secure and encrypted. Do not share information you post you can't be proud to send your identity, and may be used to target you or your loved ones in other dangerous ways. Below are some suggestions to help you manage the social networking experience safely.

DO...

- Check your friends/followers carefully. People who you know and trust could help you based on your friends and followers. Be cautious about accepting a friend request from someone you have not met in person.
- Have a reason for posting or commenting. Ask yourself: Who am I posting this? Is this something that will add value to my online reputation? Think about what you are about to share with the entire online community.
- Consider what others will think about your post. Realize that they will interpret what you say or post from the one point of view and with their own knowledge base.
- Talk about online safety with your friends and family. Be digital role models for others who are online.
- Use a strong password, at least 8 characters characters with a mixture of upper and lower case and special characters.
- Keep your social media account password separate from other accounts you have, especially for your email, banking, credit card, and investment accounts.
- Lockdown and keep up with changes in privacy settings. Social media sites are constantly changing the privacy and creating new privacy tools. Customize your personal privacy settings. Many social media sites allow you to customize your settings with different levels of privacy for different audiences.

DO NOT...

- Share confidential or sensitive information. Don't leave or form of ID, health or financial information that can be used by identity thieves. Even pictures with your home number or address can be used by scammers or other Internet criminals.
- Post anything that might be considered offensive. You need to understand and weigh the risks and consequences of sharing thoughts and ideas that might be considered offensive, or a violation of public policy.
- Share links to individuals, organizations, or groups. Law enforcement officials take the time to verify networks. You should not give links about these types of articles.
- Share information that isn't yours to share, including copyrighted material. Some mobile devices have cameras and video capabilities, it is easy to share information about other people and have your information shared. Before posting anything about someone else, ask yourself: If you would want someone to share that information about you?

CYBERBULLYING

Cyberbullying is someone who uses a computer, cell phone, smartphone or other technology to intentionally and repeatedly harass, bully or threaten another person through emails, text, social media posting, chat rooms, websites and other forms of electronic communication. Cyberbullying is most common in young people - who can participate in cyberbullying, as well. It is more likely to happen in groups than it is to happen one-on-one. The harassing person is identified and does not know their target is a person because they are not physically present to see the reactions their words cause. Because cyberbullying can happen 24 hours a day, 7 days a week, there is no end or escape for the victim. Groupthink and crowd mentality can easily occur online, with others jumping on the bullying bandwagon and their harmful words go viral.

As digital citizens, it is important that we learn to recognize the signs of cyberbullying and respond appropriately when it occurs. We have as much responsibility to look out for each other's best interest in the virtual world as we do in the real world. We should all seek to be digital role models and educate ourselves and others on appropriate online behaviors. Parents and guardians must be aware of their children's online activities and create an environment where children feel comfortable discussing cyberbullying.

Your Online Reputation

Facebook, Twitter, Instagram, YouTube, and other social networking sites have become a part of our lives. They are also a part of our online reputation. It is important to be aware of your online reputation and to create a positive one. Many organizations, such as banks, employers, and universities, can be affected by an online reputation and social media. Social networking has created many opportunities for consumers, but it must be used responsibly.

Think Long Term

Just because an online post or picture is deleted, doesn't mean that it is gone. Once something is in cyberspace, it is there forever. It is possible for other people who see it to take a screenshot or to save it for themselves. Inappropriate posts or pictures can easily come back to haunt you.

Similarly we need to think about the scope and longevity of other electronic communication, such as emails, texts or pictures. It requires little effort to forward an email, text, or picture. You never know who will eventually see or read what you have sent.

Important Password Tips

1. Create separate, unique, and strong passwords.
2. Keep your social media account password separate from other accounts you have, especially for your main email, banking, credit card, and investments accounts.
3. DO NOT use these elsewhere.

CYBER SECURITY OUTREACH

The ITT IT Division offers cyber security presentations for groups in public and community organizations. If you are interested in having an IT professional present one of these topics to your group, please email us at ITT@ttu.edu.

Cyber Security 101 (for adults who are online)

- This is your opportunity to learn the basics of keeping your personal information secure, as well as protecting your personal safety online. Topics for this presentation include:
 - Identity Theft (phishing, scams, malware, passwords, Wi-Fi, and apps)
 - Personal safety (social media, cyberbullying, and device communication)
 - Personal Responsibility

What You Need to Know About Online Reputation Management (for adults who are online)

- Posting, tagging, sharing, and retweeting have become commonplace in our society, and it is important to be aware of your online reputation and to actively manage it. Topics for this presentation include:
 - The importance of your online reputation
 - Tips for managing your online reputation
 - Lessons learned the hard way
 - Safety and creative tips for managing your online reputation

Raising Digital Citizens (for parents)

- Technology is constantly evolving, and so are the risks. This presentation provides parents with an overview of today's threats and suggestions for safely raising their children in a digital world. Topics include:
 - Online resources
 - Age-specific resources for online activities
 - Overview of apps, cyberbullying and sexting
 - General safety, awareness and protection tips
 - Online resources

Becoming Digital Citizens (for middle school & high school students)

- This presentation provides today's youth with the realities of cyber space and gives practical tips for becoming a responsible digital citizen. Topics include:
 - Questions to think about before posting online
 - Do's and Don'ts of being a responsible digital citizen
 - Discussion about apps, cyberbullying and sexting
 - Tips for general online safety, awareness and protection

Raising Cyber Literacy (for Elementary school students)

- It's important for our children to start learning about cyber space when they are young, in order for them to develop into responsible digital citizens. This presentation is an age-appropriate conversation starter to get children thinking about how to be a good "cyber citizen." Topics include:
 - Making good choices in cyberspace
 - Sexting and cyberbullying
 - Cyberbullying
 - Digital citizenship

Stranger Danger

For this project we were asked to design youth flyer's for kids from K-12 grade to be aware of strangers on the Internet. I decided to design old school 8-bit characters/objects to represent an old school computer loading screen to bring back nostalgia for older kids yet something new for the younger audience I also included a loading bar and put specific words to associate with the object presented. I used bright colors and a uniformed gradient on each different flyer to give it another unifying factor.

STRANGER DANGER

It is YOUR responsibility to practice online safety and to be a responsible digital citizen.

- Talk with your friends and family about online safety and manners, express your thoughts and listen to their concerns;
- Review your own online activity including mobile apps, sharing, posting, and images or photos—make needed changes to boost online safety; and
- Evaluate your "friends" and "followers." Never accept requests from users that you do not know—remember, you are the owner of your digital life, and you have the power to select what friends and family members participate in it.

Tips for Parents Raising Digital Citizens:

- "Friend" your child on Facebook. Follow them on Twitter. Participate in the same social media platforms as they do;
- Use everyday opportunities—such as TV shows, movies, and news stories—to discuss appropriate online behaviors and consequences of inappropriate activity;
- Stay up-to-date and informed with new technologies, up-and-coming apps and games, and privacy policies;
- Avoid oversharing about your children and family. As parents, we are creating online reputations for our children before they have a say in creating their own image on social media accounts; and
- Use your own online behavior as a role model for your family, colleagues, and friends.

Please visit www.cybersecurity.ttu.edu for more information.

Stranger Danger




Do You Know All Of Your Followers?

Everyone wants to be popular online, but this so-called "popularity" can come at a price. Allowing friends and followers into your life through social media is a very common thing, but, ask yourself, "Have I ever accepted friend or follow requests from someone who I don't actually know?" Many of us have. On top of that, how many times have we all come across profiles that end up being fake or a scam? What you allow as your friends and followers can reveal in some, or all, of your private and

personal information falling into the hands of cyber criminals. These criminals take information from your posts, pictures, and other friends' profiles and use it to gain your passwords, hack into your private accounts, or steal your identity. These are consequences that can last a lifetime. Continue to remain aware of what you're posting and who you're following. It is always okay to be cautious when it comes to who you're allowing into your life via your social media profiles!


Stranger Danger



Who Else Knows Your Password?

Passwords, Passwords, Passwords. They are a pain sometimes, aren't they? What's worse is the real life consequences you may suffer from if your password falls into the hands of a cyber criminal. Even a friend you have fallen out with, or a school buddy. A cyber criminal or hacker has the ability to use your passwords to access your personal identifiable information, steal your identity, and access all of your accounts and profiles. Others, who you may have even considered a friend at one time, could read your private messages, post and comment on your behalf, or even lock you out of your own profiles. That sounds horrible, right? Your password falling into the wrong hands has real and lasting effects on your life. Remember to always create strong password (using letters, numbers, and symbols), never share your password with others, and use different passwords for different accounts!

Stranger Danger



Do You Know Who You're Chatting With?

Face book, Message or Snapchat, and so much more! Almost every app or social media platform has the built a way to message others. Do you receive messages that seem a little odd? Even from people you do not know? It has happened to most of us, and to not that you always exercise strong password (using letters, numbers, and symbols), never share your password with others, and use different passwords for different accounts!

Never reveal your location or apps to meet up with others who have contacted you. If the person or only knows you, they likely already know your family, friends, and where you live. If someone says something that makes you feel uncomfortable, block that person immediately. Lastly, never message anything you wouldn't want the world to know! This could be your personal information, full name, phone number, school, etc., your personal thoughts or ideas that you don't want shared, or even questions/answers that could be harmful.

STRANGER DANGER

It is YOUR responsibility to practice online safety and to be a responsible digital citizen.

- Talk with your friends and family about online safety and manners, express your thoughts and listen to their concerns;
- Review your own online activity including mobile apps, sharing, posting, and images or photos—make needed changes to boost online safety; and
- Evaluate your "friends" and "followers." Never accept requests from users that you do not know—remember, you are the owner of your digital life, and you have the power to select what friends and family members participate in it.

Tips for Parents Raising Digital Citizens:

- "Friend" your child on Facebook. Follow them on Twitter. Participate in the same social media platforms as they do;
- Use everyday opportunities—such as TV shows, movies, and news stories—to discuss appropriate online behaviors and consequences of inappropriate activity;
- Stay up-to-date and informed with new technologies, up-and-coming apps and games, and privacy policies;
- Avoid oversharing about your children and family. As parents, we are creating online reputations for our children before they have a say in creating their own image on social media accounts; and
- Use your own online behavior as a role model for your family, colleagues, and friends.

Please visit www.cybersecurity.ttu.edu for more information.

STRANGER DANGER

It is YOUR responsibility to practice online safety and to be a responsible digital citizen.

- Talk with your friends and family about online safety and manners, express your thoughts and listen to their concerns;
- Review your own online activity including mobile apps, sharing, posting, and images or photos—make needed changes to boost online safety; and
- Evaluate your "friends" and "followers." Never accept requests from users that you do not know—remember, you are the owner of your digital life, and you have the power to select what friends and family members participate in it.

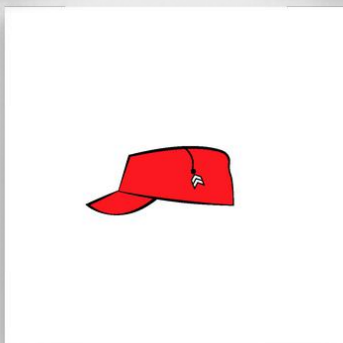
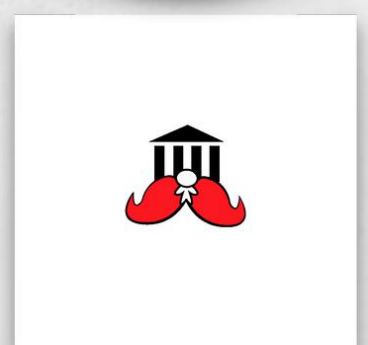
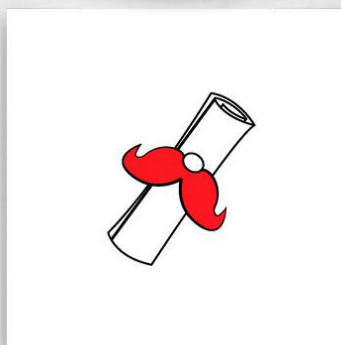
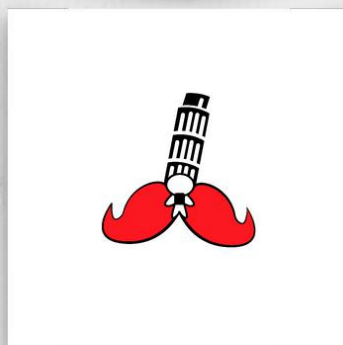
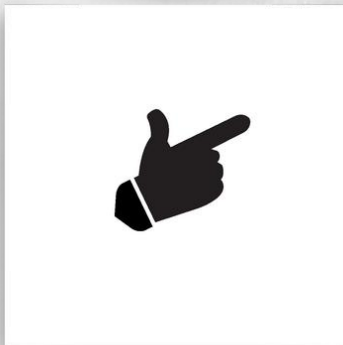
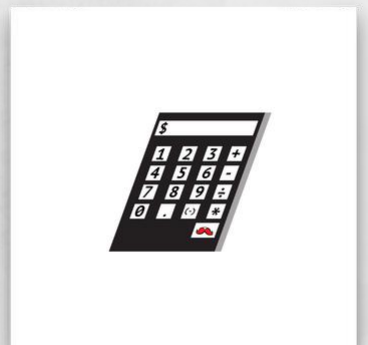
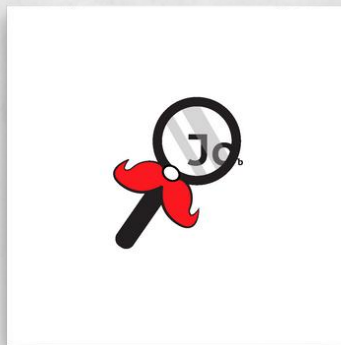
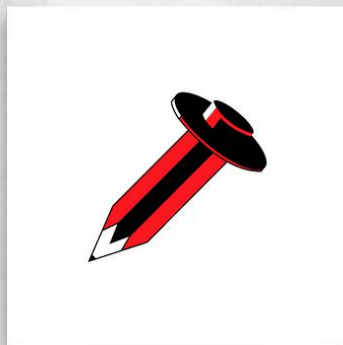
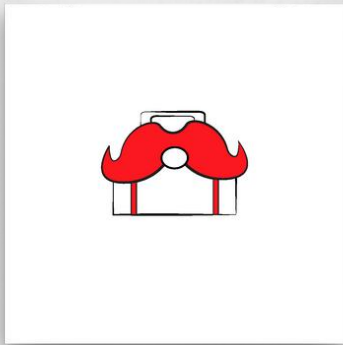
Tips for Parents Raising Digital Citizens:

- "Friend" your child on Facebook. Follow them on Twitter. Participate in the same social media platforms as they do;
- Use everyday opportunities—such as TV shows, movies, and news stories—to discuss appropriate online behaviors and consequences of inappropriate activity;
- Stay up-to-date and informed with new technologies, up-and-coming apps and games, and privacy policies;
- Avoid oversharing about your children and family. As parents, we are creating online reputations for our children before they have a say in creating their own image on social media accounts; and
- Use your own online behavior as a role model for your family, colleagues, and friends.

Please visit www.cybersecurity.ttu.edu for more information.

Survey Icons

For this project we were asked to design Icons for a survey paper so it could replace the old icons with new ones. I was given the task of making the icons Texas Tech themed and these are the ideas that I came up with. Going from top to bottom, (1. A suitcase, 2. A pencil, 3. A magnifying glass, 4. A calculator, 5. Guns up thumbs up, 6. Study aboard, 7. A diploma, 8. College, 9. Graduated veterans/soldiers) and we were only allowed to use Texas Tech approved colors.



ATLC Signs

For this project we were asked to design signs to go up around the ATLC because the ones surrounding the area were outdated and needed a new perspective. I decided to include two samples from the many signs that came out of these two themes. For the one on the top I decided to go with a geometric pattern and my inspiration was from the background I did earlier this year. For the second one I went with a more futuristic and modern look to give a new and sleek feel to the signs.



Shred Week

For this project we were given the task of creating a poster for shred week. Shred week for context is a week where students are able to go to the It department and can register to clear up old files and hard drives. What I decided to do was create an electronic grid pattern in the background to indicate a hard drive circuit but also to show that a system where students can connect through a new source.

SHRED
WEEK MARCH 25 - MARCH 28

LOTS OF OLD FILES TAKING UP SPACE?
BACK ROOM CLUTTER?

RED RAIDER SHRED WILL SECURELY DISPOSE
OF TTU DOCUMENTS AND HARD DRIVES!

STEPS

1. Register TODAY using the "Shred Week Registration" form at <https://ww.depts.ttu.edu/services/redraidershred/>
2. A Red Raider Shred representative will contact you for scheduling
3. Please ensure that all documents slated for pickup are in a sturdy lidded box, and all binders, metal fasteners (excluding staples), CDs and hard drives have been removed

TEXAS TECH UNIVERSITY
Information Technology Division

TEXAS TECH UNIVERSITY
Operations Division

ACKNOWLEDGEMENT In accordance with Texas state law, TTU (PRJ 10 and TTU (RS) OP 1005), all master copies of state records, regardless of their format, must fulfil their maximum retention time before being properly disposed. By submitting documents for shredding during Shred Week, you are acknowledging that these laws and policy requirements have been completely fulfilled. Neither Operations nor Information Technology Division will be held liable for any information or documentation that The Texas Tech University System's records retention schedule is available at <http://www.cao.ttu.edu/recordsmanagement/irs.html>. Each department should still out and maintain its own disposition log to document when master copies of records are disposed. A blank disposition form can be found at <http://www.cao.ttu.edu/recordsmanagement/abrm.html>. Further records management requires can be sent to Lynn Whitfield at lynnwhitfield@ttu.edu

