CYBERSECURITY

• BEST PRACTICES

• THE BASICS

• SECURITY & PERSONAL ONLINE SAFETY

Peggy Jones
Technology Support– Facilities and Services Manager
IDENTITY THEFT

• EXAMPLES OF PII:
  • FULL NAME
  • BIRTH DATE
  • SOCIAL SECURITY NUMBER
  • CREDIT CARD NUMBER
  • BANK ACCOUNT INFO.
  • USERNAMES
  • PASSWORDS

• METHODS TO STEAL YOUR IDENTITY:
  • PHYSICALLY STEALING YOUR WALLET OR PURSE
  • TRICKING YOU INTO SHARING YOUR INFORMATION
  • SEARCHING SOCIAL MEDIA ACCOUNTS
  • SEARCHING THROUGH YOUR TRASH
  • INSTALLING MALWARE
  • DATA BREACHES
PROTECTING YOUR INFORMATION

• INSTALL ANTIVIRUS SOFTWARE AND SET UP AUTOMATIC UPDATES

• KEEP ALL SOFTWARE UP-TO-DATE

• NEVER RESPOND TO EMAIL REQUESTS FOR PII

• LOOK FOR SECURE WEBSITES - HTTPS://WWW = SECURE

• USE CHIP-ENABLED CREDIT CARDS

• MONITOR YOUR CREDIT CARD & DEBIT BILL STATEMENTS

• USE A CROSS-CUT SHREDDER TO DESTROY PAPER DOCUMENTS
COMMON PHISHING SCAMS

• EXAMPLES
  • FINANCIAL TACTICS/GAINS - GREED
  • TOO GOOD TO BE TRUE - CURIOSITY, VANITY
  • NATURAL DISASTERS - SYMPATHY
  • DATING SCAMS - BELONGING, LOVE
  • FAKE SERVICES OR ACCOUNT BREACH - FEAR
PHISHING SCAM BREAKDOWN

- Requests for username and password, or other personal information to reset your password “for your own safety”
- Spelling & grammar mistakes
- Vague or missing information in the “From” field or email signature
- “To” field contains multiple random addresses and/or is alphabetized
- Impersonal or awkward greetings
- Unexpected attachments
PHISHING CONTINUED

- Links that are random or don’t refer to the sender
- Emails about accounts that you don’t have or from business you don’t do business with
- “From” celebrities
- Emails that sound as if they are coming from a friend, but you don’t recognize the name
- Time-sensitive threats that your account will be closed or that your email inbox is over the limit
- Gut feeling - if in doubt, always call to verify! Don’t respond to email!
MALWARE

• INCLUDES VIRUSES, SPYWARE, ADWARE, RANSOMWARE, AND KEYLOGGERS THAT CAN BE INSTALLED ON YOUR COMPUTER, TABLET, OR SMARTPHONE WITHOUT YOUR CONSENT OR KNOWLEDGE

• CAUSE YOUR SYSTEM TO CRASH, THEN GATHER SENSITIVE INFORMATION OR MONITOR YOUR WEB BROWSING TO GAIN ACCESS TO PRIVATE SYSTEMS

• PREVENTION:
  - INSTALL ANTIVIRUS & SET-UP AUTOMATIC SECURITY UPDATES
  - KEEP ALL SOFTWARE UP-TO-DATE
  - DON'T OPEN UNEXPECTED EMAIL OR FILES, OR CLICK ON UNEXPECTED LINKS
PASSWORDS

- Create unique & complex passwords for individual accounts
- Keep them private – between you & your keyboard only
- Change your passwords on a regular basis
- Avoid using personal data to create your password
- Use 1st letter of words in a phrase that is meaningful to you or Raider password guidelines
- Use a password manager:
  - KeePass (Free), LastPass, 1Password
PUBLIC WIFI

• WEIGH CONVENIENCE VS. RISK OF IDENTITY THEFT
• DON’T MAKE FINANCIAL TRANSACTIONS OR USE CREDIT CARDS
• AVOID CHECKING EMAIL ACCOUNTS OR SOCIAL MEDIA SITES
• TTU’S WIFI IS SECURE DUE TO ERAIDER LOGIN

HOME WIFI

• Change the default password
• Be careful who you share your password with
INTERNET OF THINGS

• EVERYDAY “THINGS” CONNECTED TO THE INTERNET MOSTLY TO PROVIDE A CONVENIENCE OR REMOTE CONNECTIVITY
  • TYPICAL HOME COULD CONTAIN UP TO 500 “SMART” DEVICES BY 2022
  • USE HOME WIFI OR SMARTPHONE APP, MOSTLY CLOUD-CONNECTED

• THESE “THINGS” COLLECT AND SHARE YOUR DATA
  • POSSIBLE HACKING THROUGH WIFI OR CYBERATTACKS
  • NEED TO WEIGH CONVENIENCE/ACCESSIBILITY WITH SHARING OF DATA, LOSING PRIVACY AND PERSONAL INFORMATION
INTERNET OF THINGS

- Cars with Wi-Fi, access Pandora & Google Maps, text reading features
- Remote thermostat or home security controls
- Fitbit, fitness trackers
- Voice controlled TV remote controls
- Amazon Echo or Alexa – answers questions, follows commands
- Interactive Barbie dolls and other children’s toys
- Refrigerators that track groceries & make your grocery list
- Webcams, baby monitors, nanny cams
- Others you are using or are selling in your stores?
APPS

• CAN CONTAIN MALWARE, TOO
• SHOP FOR APPS IN REPUTABLE STORES – APPLE, AMAZON, GOOGLE PLAY
• ALWAYS INSTALL UPDATES
• UNDERSTAND WHAT DATA YOU ARE GIVING THE APP PERMISSION TO ACCESS
• BE CAUTIOUS WITH APPS THAT ALLOW YOU TO SIGN IN FROM FACEBOOK
• CHILDREN SHOULD CHECK WITH PARENTS BEFORE DOWNLOADING
## Social Media Do’s & Don’ts

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Understand and keep up with changes in privacy settings</td>
<td>• Share confidential or sensitive information</td>
</tr>
<tr>
<td>• Customize your personal privacy settings</td>
<td>• Share vacation plans or photos while you are gone</td>
</tr>
<tr>
<td>• Choose your friends/followers carefully</td>
<td>• Post illegal or excessive activities</td>
</tr>
<tr>
<td>• Have a reason for posting</td>
<td>• Post negative comments</td>
</tr>
<tr>
<td>• Talk about online safety with your loved ones</td>
<td>• Post material that might be considered offensive</td>
</tr>
<tr>
<td></td>
<td>• Threaten violence to individuals, organizations or yourself</td>
</tr>
<tr>
<td></td>
<td>• Share information that isn’t yours to share</td>
</tr>
</tbody>
</table>
LONGEVITY OF ELECTRONIC COMMUNICATIONS

- JUST BECAUSE YOU CLICK DELETE DOESN’T MEAN THE CONTENT IS GONE

- EMAILS, PICTURES, TEXTS, APPS

- INTIMATE TEXTING, PICTURES OF A sexual NATURE
CYBERBULLYING

• HARASSING, HUMILIATING, TORTURING, EMBARRASSING, OR THREATENING USING DIGITAL TECHNOLOGY INCLUDING TEXTS, EMAILS, PICTURES, VIDEOS AND FAKE PROFILES

• 24/7 OF TECHNOLOGY CAN MAKE THE BULLYING POTENTIALLY MORE DEVASTATING THAN PLAYGROUND/HALLWAY BULLYING

• TECHNOLOGY OUTPACING THE LAW & SCHOOL POLICIES
WHAT CAN WE DO?

• TREAT OTHERS THE WAY WE WANT TO BE TREATED
• BE DIGITAL CITIZEN ROLE MODELS FOR OUR CHILDREN AND PEERS
• STOP SHARING, COMMENTING, AND FORWARDING INFORMATION ABOUT OTHERS JUST TO GET A LAUGH
• REMEMBER WHEN WE ARE COMMUNICATING OR SHARING ONLINE THAT THERE IS A PERSON BEHIND THE SCREEN OR THE PICTURE
CYBER SECURITY IS EVERYONE’S RESPONSIBILITY

• BE AWARE OF CURRENT SCAMS. HAVE A HEALTHY SUSPICION.
• ACTIVELY THINK ABOUT YOUR ONLINE ACTIONS.
• REAL LIFE CONSEQUENCES TO VIRTUAL ACTIONS.
• JUST BECAUSE YOU CAN, DOESN’T MEAN YOU SHOULD.
• TALK OPENLY WITH LOVED ONES AND FRIENDS – ESPECIALLY THOSE WHO ARE NEW TO TECHNOLOGY AND DEVICES.
CYBER SECURITY BOILS DOWN TO

COMMON SENSE
ACCOUNTABILITY
PERSONAL RESPONSIBILITY
RESOURCES

• [WWW.CYBERSECURITY.TTU.EDU](http://WWW.CYBERSECURITY.TTU.EDU)

• [ONGUARDONLINE.ORG – FACEBOOK FAN PAGE](http://ONGUARDONLINE.ORG)

• [STOPTHINKCONNECT.ORG](http://STOPTHINKCONNECT.ORG)

• [STAYSAFEONLINE.ORG](http://STAYSAFEONLINE.ORG)

• [FACECROOKS – FACEBOOK FAN PAGE](http://FACECROOKS)