

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](https://www) = S  E = 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



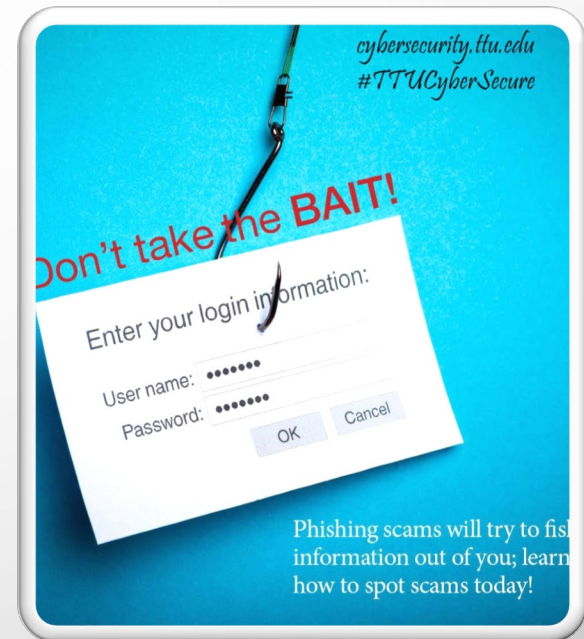
PHISHING SCAM BREAKDOWN



- 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!



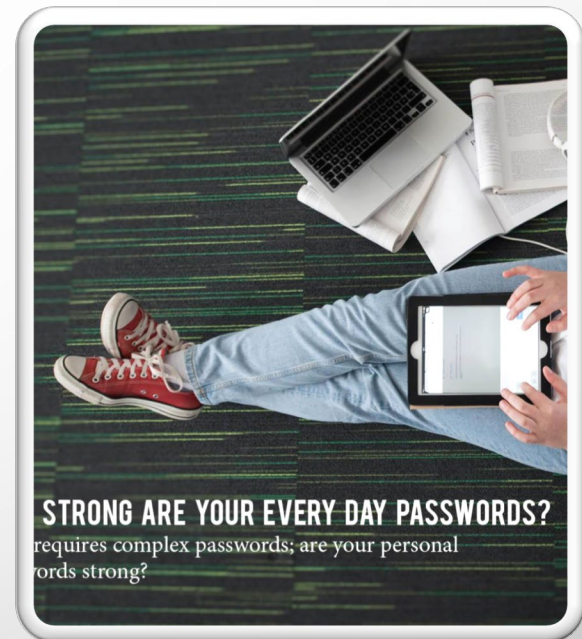
MALWARE



- 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 ERAIDER PASSWORD GUIDELINES
- USE A PASSWORD MANAGER:
 - KEE PASS (FREE), LAST PASS, 1 PASSWORD



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 WIFI, 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

DO'S

- UNDERSTAND AND KEEP UP WITH CHANGES IN PRIVACY SETTINGS
- CUSTOMIZE YOUR PERSONAL PRIVACY SETTINGS
- CHOOSE YOUR FRIENDS/FOLLOWERS CAREFULLY
- HAVE A REASON FOR POSTING
- TALK ABOUT ONLINE SAFETY WITH YOUR LOVED ONES

DON'TS

- SHARE CONFIDENTIAL OR SENSITIVE INFORMATION
- SHARE VACATION PLANS OR PHOTOS WHILE YOU ARE GONE
- POST ILLEGAL OR EXCESSIVE ACTIVITIES
- POST NEGATIVE COMMENTS
- POST MATERIAL THAT MIGHT BE CONSIDERED OFFENSIVE
- THREATEN VIOLENCE TO INDIVIDUALS, ORGANIZATIONS OR YOURSELF
- SHARE INFORMATION THAT ISN'T YOURS TO SHARE

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, TORMENTING, 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.



The background of the slide is a light gray gradient with several realistic water droplets of various sizes scattered across it. The droplets have highlights and shadows, giving them a three-dimensional appearance. The text is centered on the slide.

CYBER SECURITY BOILS DOWN TO

COMMON SENSE
ACCOUNTABILITY
PERSONAL RESPONSIBILITY

- WWW.CYBERSECURITY.TTU.EDU
- ONGUARDONLINE.ORG – FACEBOOK FAN PAGE
- STOPTHINKCONNECT.ORG
- STAYSAFEONLINE.ORG
- FACECROOKS – FACEBOOK FAN PAGE

RESOURCES