Cyber Security

Maintaining Your Identity on the Net
Why Cyber Security?

- There are three points of failure in any secure network:
  - Technology (hardware and software)
  - Technology Support (ITS)
  - End Users (USD students and employees)
- Technology can be upgraded and Technology Support can be trained, but only you can make safe decisions on the Net!
Why Was I Hacked?!

- Most hackings are non-personalized and semi-malicious
  - E.g. Mass brute-force hackings, phishing attempts, and spyware
  - These attacks are concerning, but often times are more annoying than dangerous
  - Often, the end goal of non-personalized attacks is to advertise through spam

- Some attacks are non-personalized and highly malicious
  - E.g. Fake Anti-viruses, data-destructive infections, Ransomware, and some phishing attempts
  - These infections are often trying to exploit end users for profit, steal generic identities, and cause data destruction for “fun”

- Few attacks are personalized and highly malicious
  - Spearphishing is targeting a single company or institution for a specific goal
  - Often includes Social Engineering, or non-technological hacking
  - USD was Spearphished in March of 2016
Security Basics - Your Password
Components of a Secure Password

- **Length** - 10 or more characters, minimum!
  - Length is the most important component of password security
  - A randomly generated, 10 character password using only lowercase letters is exponentially more secure than a 6 character password using caps, special characters, and numbers

- **Non-dictionary words**
  - Brute-force cracking a password is slowed considerably by using non-words
  - An easy way to do this is by using acronyms

- **Non-personal words**
  - Social engineers can easily investigate your address, pet’s name, and children’s birth date
  - Using acronyms or combining personal data can help avoid this
Secure Passwords, cont’d

- Special Characters
  - Unique characters like $ or @ add variables that make brute force hacking harder
  - Special characters are important, but not as important as character count

- Capitalization/Numbers
  - Numbers and capitals add variables like special characters
  - Like special characters, character count is more important

- Memorability
  - The least secure password is one that you can’t remember and write down
  - An easy way to memorize is practice typing your password - muscle memory is strong!
Password Tips:

- Try to avoid using the same password for accounts of differing importance
  - Using the same password for Facebook and Twitter is fine
  - Using the same password for Facebook and your bank account is **insecure**
- Don’t write your password down!
  - Keeping passwords documented in a locked document or password manager is fine
  - Writing passwords on post-its and keeping them on your desk is **insecure**
- Try using acronyms and variations
  - E.g. “My daughter’s favorite toy is her sonic screwdriver” becomes mdfthss
  - This can then be expanded upon: Md ft_!h$$
- Spaces usually count as characters too - phrases can be extremely effective
Malicious Software
How it works and how to recognize it
Spyware

- Spyware is a type of malicious software specifically used to send information from a host computer to the owner of the Spyware.
- Spyware is often used for advertisements, acquiring of personal information, and documenting computer activity.
- Spyware often lurks in toolbars and browser add-ins.
- Often, Spyware is less detectable than other Malware - it wants to stay hidden, not cause chaos.
- Keyloggers are a subtype of Spyware - they are used to track what is typed on the computer and send it back to the owner of the program.

KEYLOGGERS CRACK PASSWORDS
Example - Browser Toolbar Spyware
Viruses and Malware

- Viruses and Malware are malicious software designed to cause damage or data loss on computers.
- Some Malware tries to exploit users into paying the host company to remove its own software.
- Some Malware emulates Anti-Virus (AV) programs. If you don’t remember installing an AV, it might be Malware!
- Since Malware can cause data loss or computer damage, it is important to head these infections off as soon as possible!
Example - Fake Antivirus Program
Ransomware

- Ransomware is specialized Malware that encrypts all files on a computer with a randomly generated key that must be purchased from the provided company.
- In some instances, as with Cryptolocker, this key is deleted after three days, at which point the data becomes irretrievable.
- Usually, data destruction by Ransomeware is not reversible; the best way to avoid data loss is to avoid infection through safe browsing.
Example - Cryptolocker

![Cryptolocker screenshot]

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, video, documents, etc. HERE is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key will allow you to decrypt the files on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR, similar amount in another currency.

Click Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.
Scams and Techniques
What to look for and what to avoid
Phishing

- **How Phishing works:**
  - Phishing occurs when a fraudulent source requests your username and password for any reason
  - Once the username and password have been entered, this information is sent to the fraudulent source, and your credentials have been compromised

- **How to avoid getting Phished:**
  - Legitimate sites will rarely provide you a link to reset your password unless you have requested one
  - USD will NEVER request your credentials via email
  - Never hesitate to call for confirmation - the Help Desk can help you determine whether an email is legitimate or not
Phishing Examples

Example 1

University of San Diego <brobertson@stmartin.edu>
E-Notification of Your Payroll 2016

Dear Member,

You have 1 new
Click Here To Renew

Regards,

IT Help Desk

© 2016 University of San Diego

- Undefined recipients
- Questionable salutation
- Highly suspicious URL revealed when hovering over the embedded link.
- Payroll topic would never come from ITS HelpDesk
- Domain name: Why would anyone from stmartin.edu ever email you about USD payroll matters?
- No specific contact information (ITS HelpDesk individual)
I need you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF send as attachment. Kindly prepare the lists and email them to me asap.

Regards

James
Unsolicited Support Calls

- Sometimes, scammers will contact users under the pretense of a support call from Microsoft
- Be warned - Microsoft rarely, if ever contacts customers directly without solicitation
- If the caller ever asks for personal information, a credit card number, or permission to control your computer, make sure you can verify the identity of the caller first!
  - Pro Tip: ITS employees will always have a Ticket Number to associate with your computer, and we will always introduce ourselves in a way that can be verified by the USD website!
- If you are ever suspicious of whether a call is a scam or not, tell them you will call back at the number provided on the company website
Social Engineering

- Social Engineering is exploiting social rules and expectations to gain access to confidential information.
- Social Engineers focus gathering personal information about a company or employee to guess passwords or exploit security loopholes.
- Under most circumstances, Social Engineers target high-profile companies or individuals to access information, money, or power.
- The best way to protect against Social Engineers is to follow safe protocol and to always ask questions:
  - Never give your password over the phone if a technician insists.
  - Don’t be afraid to question why information is requested or to contact ITS if something sound suspicious.
Safe Browsing Techniques

Almost all infections are contracted from the Net, and almost all infections can be prevented by following safe browsing techniques while online.

- Never click ads - if you are interested in a product in an ad, search for the website in Google. Clicking an ad can redirect you to malicious website.

- Websites or programs offering “free smileys,” “free games,” “free fonts,” or other aesthetic changes to your machine often come loaded with spyware - beware, or ask the Help Desk.

- **Check the URL!** If a website for Bank of America asks you to log in, but the URL doesn’t say Bank of America, it is likely a Phishing Attempt.
  - Pro Tip: look for the [address].[address].com/org/edu; if this part of the URL is fishy, then it’s probably illegitimate!

- Watch out for pop-ups. If you are getting frequent pop-ups, you may already be infected, or the page you are on may have malware.
Safe Browsing Techniques, cont’d

- Avoid ads that look like Windows Update links - if you didn’t seek out the “update,” don’t install it
- Make sure to read the checkboxes during software installation - many programs include bloatware (unnecessary software that slows down your computer)
- Google unfamiliar programs or pop-ups to see if they are Malware
- Use high-profile websites, like Amazon, Google, Bing, and Yahoo
- Watch out for redirects! If you go to a familiar site like Google, and are redirected somewhere else, you might be infected
- Play it safe - it’s always easier to ask before you click than to remove Malware!
Protecting Yourself

- Download and install your Microsoft Updates (for Windows) and Software Updates (for Mac)!
- Ensure you have antivirus software installed and updated
  - USD provides you with Symantec Endpoint Protection by Norton Security, free of charge!
- Be aware of pop-ups, changed home pages, locked files, and other unusual activity on your computer
- Never hesitate to call or email and ask questions.