Confidential Data Handling Techniques

Office of the Vice President for Information Technology
Ms. Lori McElroy, Information Security Officer

TEXAS STATE UNIVERSITY
SAN MARCOS
The rising STAR of Texas

Agenda

- Identify and Classify Confidential Data
- Secure Data Handling
- Best Practices for Securing Information
  - Mobile computing
  - Wireless networks
  - Passwords
  - Internet browsing
- Identity Finder

What is Confidential data?

- State of Texas definition:
  "Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements)."

Confidential information data classification

http://security.vpit.txstate.edu/policies/data_classification.html

Public information	• e.g., job postings, service offerings, published research, directory information, degree programs.
Sensitive information	• e.g., performance appraisals, dates of birth, and email addresses), donor information.
Confidential/ Restricted information	• e.g., SSN, credit card info, personal health info.

Storing Confidential data

- Servers, file shares, secured databases in the Data Centers - YES
- Workstations, laptops - NO
- Removable media (USB, DVD, external drive) - NO
- Smart phones and other devices – definitely NOT

Storing Confidential data

UPPS 04.01.01 states that Confidential information:

- …should not be stored on portable or personally-owned devices and media unless encrypted
- …should not be stored on any device external to the campus network (e.g. cloud services)
- …must not be transmitted unencrypted over a public network (e.g. email)

Storing Confidential data

Confidential information:

- …must not be accessed from remote locations except in an authorized manner (e.g. VPN)
- Payment cardholder data shall not be stored on any device connected to the university's data network for longer than is necessary to authorize a transaction using that information.

Sharing Confidential data

- Secure file shares and databases in the Data Center (e.g. SAP, Banner, department share) - YES
- Encrypted USB or external drives - YES
- Email – NO (keep personal mail separate)
- Unsecured websites (http) - NO
- Texting - NO
- Unencrypted USBs or DVD/CDs Nope

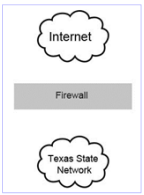
What are the risks?

- Loss or leakage of confidential data can lead to:
  - Compliance violations, PCI, HIPAA, FERPA
  - Identity theft
  - Degradation of University and System reputation
  - Financial
- Average cost of data breach in US for Higher Ed = $203/record (ex: 1000 records exposed cost over $200,000)

http://security.vpit.txstate.edu itsecurity@txstate.edu

How Texas State protects our information

- Perimeter security devices
- Anti-virus software for laptops/desktops
- Automatic system updates for laptops/desktops
- Provide secure file shares
- Encryption solutions
  - Contact IT Security



Your role in protecting our information

- Read and understand our policies
  - UPPS No. 04.01.01, Security of Texas State Information Resources
  - UPPS No. 04.01.05, Network Use Policy
  - UPPS No. 04.01.07, Appropriate Use of Information Resources
  - UPPS No. 05.01.02, University Surplus Property
- Treat data like it's your personal information
- Refer to handout "Data Security Checklist"

Your role in protecting our information

- If you access the university network remotely, use our VPN
  - To setup remote desktop: www.tr.txstate.edu/get-connected/computerservices/remote-desktop-setup
  - To access the VPN: https://ive1.txstate.edu
- Use best practices for…passwords, downloading, browsing the Internet

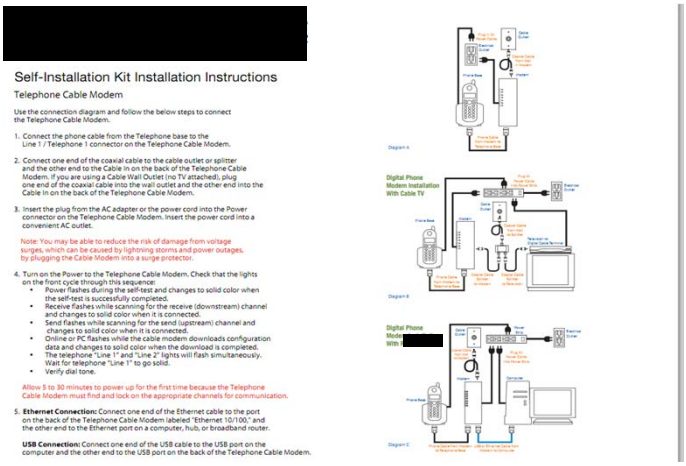
Mobile computing

- Use passwords on all mobile devices
- Always keep the device with you when you are away from the office
- Disable unnecessary services (Bluetooth, Location Services)
- Use an encrypted USB device
  - IronKey, Aegis external encrypted
- Remove or "shred" all data before disposing or transferring your [smart]phone

Wireless network security

- At Texas State
  - Encrypted wireless network setup: www.tr.txstate.edu/get-connected/computerservices
- Change your router's default password
- Use the strongest encryption available
  - WPA or WPA2
- Avoid public, open, "free" wireless networks (e.g. hotels, airports, coffee shops, your neighbor's) unless you use a VPN

Internet access at home…be careful



Self-Installation Kit Installation Instructions

Telephone Cable Modem

Use the connection diagram and follow the below steps to connect the Telephone Cable Modem.

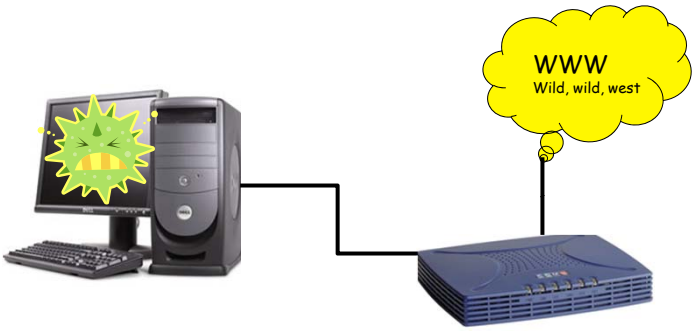
1. Connect the phone cable from the Telephone base to the Line 1 / Telephone 1 connector on the Telephone Cable Modem.
2. Connect one end of the coaxial cable to the cable outlet or splitter and the other end to the Cable In on the back of the Telephone Cable Modem. If you are using a Cable Wall Outlet (no TV attached), plug one end of the coaxial cable into the wall outlet and the other end into the Cable In on the back of the Telephone Cable Modem.
3. Insert the plug from the AC adapter or the power cord into the Power connector on the Telephone Cable Modem. Insert the power cord into a convenient AC outlet.

   Note: You may be able to reduce the risk of damage from voltage surges, which can be caused by lightning storms and power outages, by plugging the Cable Modem into a surge protector.
4. Turn on the Power to the Telephone Cable Modem. Check that the lights on the front cycle through this sequence:
   - Power flashes during the self-test and changes to solid color when the self-test is successfully completed.
   - Receive flashes while scanning for the receive (downstream) channel and changes to solid color when it is connected.
   - Send flashes while scanning for the send (upstream) channel and changes to solid color when it is connected.
   - Online or PC flashes while the cable modem downloads configuration data and changes to solid color when the download is completed.
   - The telephone "Line 1" and "Line 2" lights will flash simultaneously. Wait for telephone "Line 1" to go solid.
   - Verify dial tone.

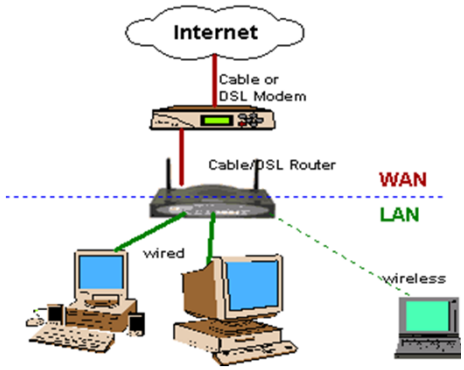
   Allow 5 to 30 minutes to power up for the first time because the Telephone Cable Modem must find and lock on the appropriate channels for communication.
5. **Ethernet Connection:** Connect one end of the Ethernet cable to the port on the back of the Telephone Cable Modem labeled "Ethernet 10/100," and the other end to the Ethernet port on a computer, hub, or broadband router.

   USB Connection: Connect one end of the USB cable to the USB port on the computer and the other end to the USB port on the back of the Telephone Cable Modem.

Surfing at home…what not to do



Wireless at home…done right



Phishing

- Protect yourself:
  - Avoid clicking on links in unfamiliar email
  - Never submit personal information in response to an email, even if it's from IT ☺
  - Verify the authenticity and security of web sites before entering your personal information (https, certificate)
  - http://security.vpit.txstate.edu/awareness/phishing

Accounts and Passwords

- Use strong passwords
  - Use passphrases
  - The longer the better, but a minimum of 8 characters
  - Mix upper case, lower case, and numeric characters
  - Avoid using personal information (i.e. your birth date, children's names)

Password "System"

i love to fly fish in montana in the summer time

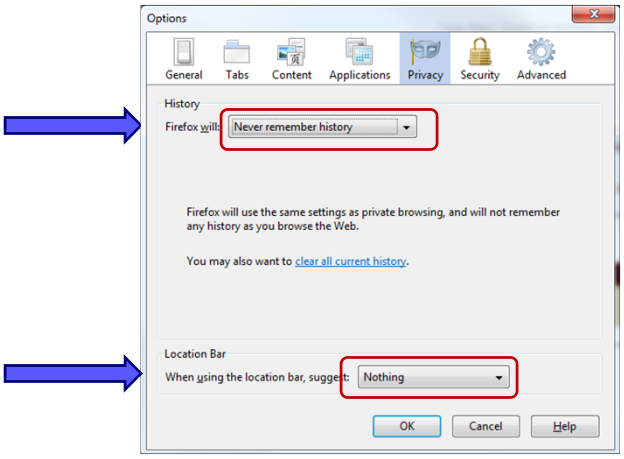
IEoyhn@nere|yah|601

Base | URL | Number to decrement

- Use the last letter of every word
- Capitalize the first two characters of your base password
- Use an @ for every "a"
- Add first three characters of url or function of each website you visit
- Use an incremental numbering scheme for password changes

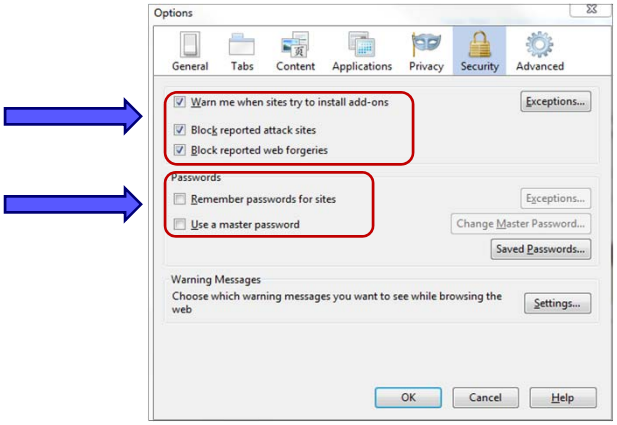
Browser Security-Firefox

Tools -> Options -> Privacy



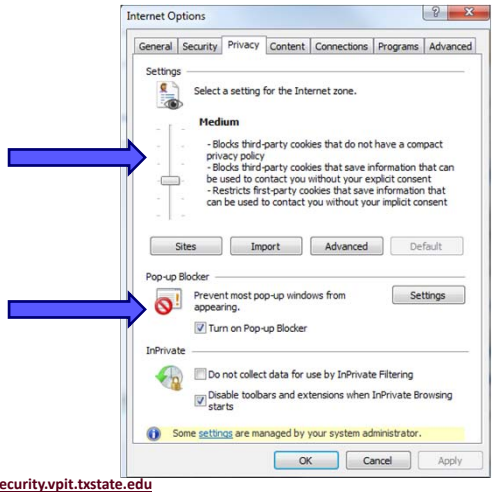
Browser Security-Firefox

Tools -> Options -> Security



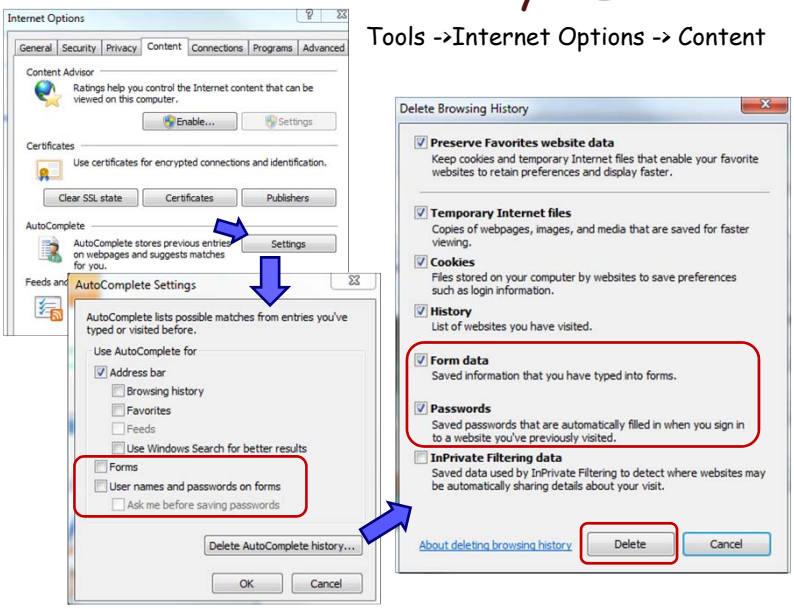
Browser Security-Internet Explorer (IE)

Tools ->Internet Options -> Privacy



Browser Security-IE

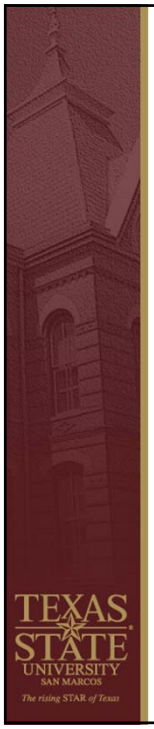
Tools ->Internet Options -> Content



Confidential Data Discovery

- Identity Finder
  - Discovers SSNs, Credit Card numbers, passwords
  - Provides a secure method of removal
  - Easy to use interface
  - Recommend to run weekly
  - Free home version

identityfinder



Contact

IT Security
itsecurity@txstate.edu
245-4225

Lori McElroy
Lori.mcelroy@txstate.edu
245-7885