



PRAIRIE VIEW A&M UNIVERSITY

October is...
Cyber Security
Month



Topics



- Passwords
- SPI (Sensitive Personal Information)
- Emails
- Access Control
- Portable devices
 - (Mobile, Thumb, laptop, iPad, Tablet, etc)
- Social Media
- Check your password

Passwords

How do I make a strong password?

- What do I use?
 - Upper Case Letters
 - Lower Case Letters
 - Numbers
 - Special Characters
 - Minimum of 8 Characters
 - No Dictionary Words
- For Example:
 - At least **2** upper case letters (A-Z)
 - At least **2** lower case letters (a-z)
 - At least **2** numbers
 - At least **2** special characters (*\$#-^)

*Note: You should **NOT** start or end your password with numbers or special characters.

Examples of STRONG passwords

- **Think of a phrase or sentence that's easy for you to remember.**
 - **“Look before you leap”**
 - Lb4u!3@P
 - **“My Brother is 18 at California!”**
 - BR18@c!a

DO NOT use

In any form do not use

- Fall20__!
- Summer20__!
- Winter20__!
- Spring20__!
- ChangeMe_
- Welcome_
- Password123
- P@ssword1
- Pvamu_ _ _
- Panther_
- PV_ _ _ _ _

Why do I want a Strong password

- Your password is to secure access to your information
- Your grades, your refunds, your personal information, your class work, your private emails, maybe even some of your parents/spouses information



Hmmm? What can I do with your information?
LOTS!

- I can get credit for your ideas
- I can share or sell your personal information
- (Student) I can steal your refund
- (Faculty) I can affect your job by posting my own grades as well as my classmates

Sharing your Password?

1. DON'T share your password with others.
2. If a helpdesk employee or anyone helping you with your password and ask for your password, ask for theirs if they aren't willing to share should you? NO!
3. Refer back to number 1



SPI

(Sensitive Personal Information)

- What is it?
 - An individual's name, address, or telephone number combined with any of the following:
 - Social security number or taxpayer ID number
 - Credit or debit card number
 - Driver's license number
 - Date of birth
 - Medical or health information protected under HIPAA
 - Student related data protected under FERPA
- Why do I care?
 - It is the law
BUSINESS AND COMMERCE CODE
TITLE 11. PERSONAL IDENTITY INFORMATION
SUBTITLE B. IDENTITY THEFT
CHAPTER 521. UNAUTHORIZED USE OF IDENTIFYING INFORMATION
 - It is a difficult task to stop credit cards and prove you didn't spend the money
 - You may end up owing money that you haven't spent

Email Phishing

Phishing scams

- PV will never ask you in an email:
 - Social Security Number
 - Date of Birth
 - Your Password
 - Your User Name or ID
 - Credit/debit card number
- **Never respond to an email requesting the above or other personal information, no matter how official it looks.**

Outside Companies

- Most companies will NEVER ask you for your password in an email, call them and verify that they sent the email if you do.
- If you receive an email asking for you to reset your password, do not use the link provided in the email. Links given to you means you could end up on a fraudulent site. Go to the company's password change tool.

Something Phishy to think about.

- ❖ An [Intrepidus Group](http://www.esecurityplanet.com/views/article.php/3875866/Top-Ten-Phishing-Facts.htm) analysis of 69,000 workers around the world found that 23 percent fell for spear phishing scenarios.
<http://www.esecurityplanet.com/views/article.php/3875866/Top-Ten-Phishing-Facts.htm>.
- ❖ Over 500 million phishing emails appear in inboxes every day
http://www.wombatsecurity.com/assets/files/PhishPatrol%20White%20Paper_April%202012.pdf
- ❖ Every year thousands, if not millions, of people fall for phishing scams
<http://techknowledgetoday.blogspot.com/2012/08/what-is-phishing-part-1-online.html>
- ❖ **Phishing is their job they become experts.**

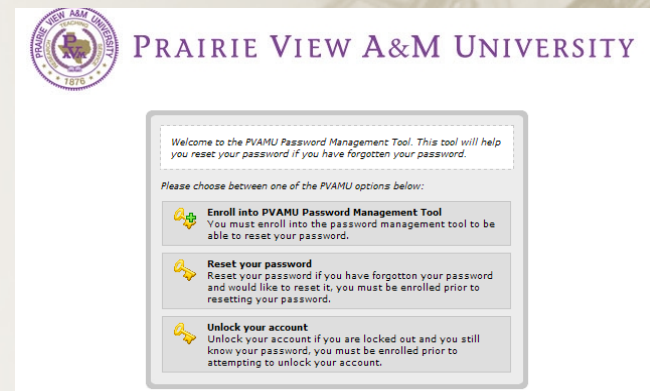
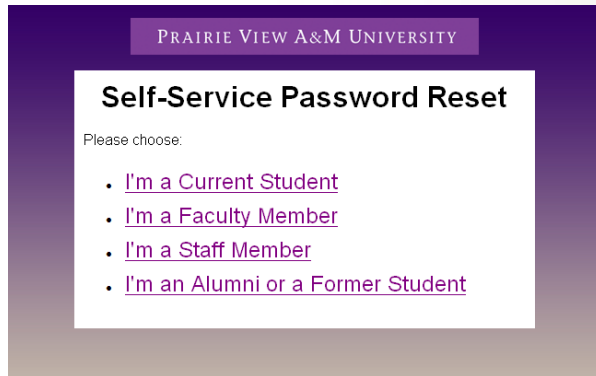
Sample Phishing Email

- *From: laila el ghalemi [mailto:promo_car@menara.ma]*
- *Sent: Tuesday, October 23, 2012 11:31 AM*
- *Subject: ATTN*
- This is from the email account investigation agency, we where set up by the *U.N* working under the CIA (Central Intelligence Agency) Bodies, our *duties is to* monitor and investigate email addresses *and mails* to prevent individuals from getting scam.
- You are hereby required to forward to this office via email emailinvestigationteam1@yahoo.com.hk every *mail* and content of anyone you are dealing any transaction with online or paying money to, or any email you suspect to be scam, so we can investigate them and let you know the legitimacy, and if *any is to be Fraudulent*, we shall immediately send the FBI after them, and charge them for *Fraud*
- Our duties is to fight against scam and terrorism.
- Thanks
- *Yours Sincerely*
- *Capt. Jeffry Adams*
- *Investigation officer*

PV Password tools

- **Password Management Tool**

- Panthertracks (top of PV home page)
- Current Students
- Password Management Tool
 - Who are you?
- Note: Staff
 - Must enroll in tool **prior** to being locked out or password expiring.



PV Password tools (continued)

- **Ctrl+Alt+Delete**
 - Once **YOU** are logged onto the PV network (on campus computer) this option is available
 - Change password
 - Old password
 - New password
 - Confirm the new password
- **In person (with picture ID) if the other options didn't work**
 - S.R. Collins Room 106
 - Monday – Friday 8am-4pm
 - Distance Learning may call 936-261-9300 (Monday – Friday 8am-4pm)

Access Control

Don't sign on for someone else.



YOU will be held accountable.

Sign off when your done.

To Lock the Computer

- Press the Windows+L key on the computer keyboard.



- Lock the computer when you need to step away in an unsecured area.

Portable devices

(Mobile, Thumb, laptop, iPad, Tablet, etc)

- Keep track of your portable device(s), especially those flash drives
- Password protect each device
- **Back up** anything that's important to you.
 - Papers/essays, Projects , Research data , Pictures, Music files, and more...

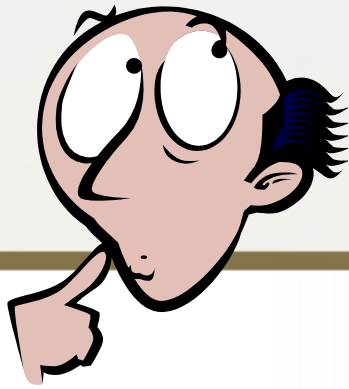
Social Media Can...

(Facebook, Twitter, LinkedIn)

- Accidentally expose personal/confidential information
- Lead to copyright infringement
- Keep in mind. . . your online activity is not anonymous and it is traceable
- Expose your computer to malware

Check your password

- We have a few computers for you to do this now at the back of the room.
 - <https://www.microsoft.com/security/pc-security/password-checker.aspx>
 - <http://www.passwordmeter.com>



THINK BEFORE
YOU CLICK!

PRAIRIE VIEW A&M UNIVERSITY

Questions?



PRAIRIE VIEW A&M UNIVERSITY



Contact Information

**Information Security
Officer**

936-261-2126

PRAIRIE VIEW A&M UNIVERSITY