SECURITY AWARENESS WHILE WORKING REMOTELY

CENTER FOR INFORMATION TECHNOLOGY EXCELLENCE (C.I.T.E.)



Agenda

- 1. Importance why?
- 2. Core Security Risks
- 3. Security Awareness In Your Home Environment
- 4. Working From Home Securely
- 5. Secure Video Conferencing
- 6. Personal Computers and Updates
- 7. Security Team



Importance - Why?

- Things we need to know to secure work from home environments during the Covid-19 pandemic and beyond.
- Employees are going through a great deal of both stress and change.
- Adapting to a new environment.
- We are all targets!



Core Security Risks



Social Engineering

- 1. <u>Questionable Request</u>: Someone asking for information they should not have access to or should already know.
- 2. <u>Pay attention to emails</u>: Look at the sender, look out for emails impersonating PVAMU employees, always look for grammatical errors.
- **3.** <u>Urgency/Protocol</u>: Someone pressuring you to ignore or bypass our security policies and procedures.
- 4. <u>Resist the Rush</u>: Someone creating a tremendous sense of urgency. If you feel like you are under pressure to make a very quick decision, be suspicious.
- 5. <u>Think Before You Click</u>: Someone wants you to carelessly click on links and not think twice before opening attachments. <u>Be cautious</u>: one wrong move could infect your device and spread it to others. Hover over the links to see where links are really going.



Social Engineering

- 6. <u>Don't Just Download It or Plug It In</u>: Someone is counting on you to download unapproved software or plug in infected USB drives or external devices. Only use authorized hardware and software.
- 7. <u>Recognize the 'Bag of Tricks'</u>: Something too good to be true. A common example is you are notified you won the lottery, even though you never even entered it.
- 8. <u>Ask Questions, and If It Feels Odd or Suspicious, Contact Security</u>: If you feel you are experiencing a social engineering attack, hang up the phone (or do not respond to the email), and contact security right away.

<u>Remember that we are not trying to get you, we are trying to help you.</u>



Sample Phishing Email

- From: ITS TEAM [mailto:ITSteam.pvamu@gmail.com]
- Sent: Wednesday, January 16, 2019 10:27 AM
- To: Jones, Yolanda <yrjones@pvamu.edu>
- Subject: Your Email Address is set to be Deactivated
- Hello,
- This message is to inform you that your email address (harose@pvamu.edu) was recently discovered to be sending spam emails to government computer systems.
- In order to prevent your email account from being deactivated we need to you to verify that you are in fact the owner.
- Please visit <u>this site</u> to verify that it is an active email address and not a part of spamming activities.
- Your prompt compliance with this notice is appreciated. No action will result in your email address being disabled.
- Thank you,
- ITS Team

http://www.pvamuedu.mydesign.com



Phishing email test: <u>https://phishingquiz.withgoogle.com/</u>

Phishing website test: <u>https://www.opendns.com/phishing-quiz/</u>



Be Cautious:

- Do not open unexpected attachments
- Never enable Macros unless you know who created the document
- Do not click on unknown file extensions



Passwords

Tips for Secure Passwords

- Old Standard 8 characters containing upper case, lower case, special characters, numbers, change every 90 days. Tip- an 8 charcter password can be compromised in less than 4 hours
- 2. New Standard 12-16 characters containing upper case, lower case, special characters, numbers, change every 2 years.
- Use multiple small words (3 or more) not complete sentences to make a passphrase – e.g. TwoTooTo@22To. <u>DO NOT</u> use common phrases from movies or books



Passwords

- 1. Never save a password in your browser, always use a password keeper PVAMU has purchased Lastpass for all faculty, staff and students. (Pvamu.edu/Lastpass)
- 2. Never share passwords you are responsible any activity completed under your account
- 3. Create a unique password for each account.
- 4. Never use public computers to log in to your online accounts.
- 5. Use two-step verification (DUO) whenever possible.
- 6. Do not use your PVAMU password on any other site Keep work and personal life separate.





Security Awareness In Your Home Environment

- Look out for phishing emails and sites. You will be targeted!
- Beware of remote desktop inquiries do not grant anyone control of your desktop unless you initiated contact with the user.
- Never provide your passwords to anyone through email or over the phone, PVAMU will not request your password.
- If you did not initiate a ticket for help, do not answer the call from non PVAMU phone numbers.
- Issues with your video conference Ensure no one else is on your network watching video, playing video games, etc. (Creates a negative impact.)
- All websites where data is entered should contain https:// at the beginning, e.g. https://www/pvamu.edu



Working From Home Securely

- You Be Cognizant of surroundings and bystanders!
- Home Network secure you Wi-Fi access point/router.
- Restart your routers/modems often.
- Family and Guests should not access work related devices.



- Passwords use strong passwords- change default passwords to strong passwords.
- Keep a separate network for guest and a separate network for family.
- Only utilize VPN when it is necessary e.g. accessing FAMIS, BANNER, Departmental Shares, when travelling.
- Utilize Syncplicity to access files / store sensitive files.
- Avoid the use of unencrypted USB sticks only use approved university USB devices.
- Keep an eye on your device never leave it unattended, lock you machine if at home, if you are in public, always power down your computer when not in use.
- Be careful of using WiFi at a family members house or free WiFi at a public location- use VPN to protect your data, the network you use may be compromised.

Secure Video Conferencing

- Do not post Zoom/WebEx/Teams links on other sites (Only in eCourses or through PVAMU official email).
- Meetings should be private not public.
- When creating a meeting, always require a password.
- Do not allow the meeting to start unless host arrives create a meeting room.
- Perform a virtual role call / Use the waiting room feature if possible.
- Lock the meeting once everyone is in Be sure to let one user in at a time.
- Be careful of what is in chat.
- If audio is breaking up, dial by phone and use the video to view the presentation.
- Enable host only sharing. If other users are allowed to share their screens to present to everyone else, grant the users the permission to share only when required.
- Be careful of fake emails or popups instructing you to install Zoom/WebEx/Teams, these should only be installed legitimate sources e.g. Zoom should only be installed by going to https://pvpanther.zoom.us/
- If you receive a request to support you, please be sure that this is a prearranged meeting with your support personnel. The request should come from a PVAMU user and from an official PVAMU account.



Personal Computers and Updates

We strongly encourage you never to use your personal computer for work, that includes logging into single sign on but if you do, please keep the following items in mind:

- Use the VDI where possible.
- Keep your operating system and antivirus up to date by turning on automatic updates.
- Do not use outdated applications, always keep them updated from legitimate sites such as from the manufacturer.
- Be careful of phishing links coming to your personal email educate your family. It only takes one person on a computer to click a phishing email and compromise everyone.
- Keep your cell phones and mobile apps up to date beware of free apps that steal information downloaded to your phone including university data.
- Beware of free movie sites or sites that give you a pop up to install software.
- Strongly recommend Use 2 factor authentication on every account you have, i.e. bank acct, etc.



Security Team

Help Desk

For general troubleshooting such installing software or applications not working correctly, please contact X2525 or <u>servicedesk@pvamu.edu</u>

Incident Reporting

If you have clicked on a link in a suspicious email or opened a suspicious attachment, or if you notice unusual pop ups and activity on your computer, contact <u>informationsecurity@pvamu.edu</u>





C.I.T.E. Resources

Telecommuting Page

pvamu.edu/telecommuting

Training Page

pvamu.edu/ITS/training

	🖾 🖓 de a Starth	Q	C Search Q
PRAIRIE VIEW ARM UNIVERSITY STUDENTS FLOUTY AND STAFE PARENTS AND FAMILY ALUMI			STUDENTS FACULTY AND STAFE PARENTS AND FAMILY ALUMNI
APPLY NOW ABOLT PNAMU ADJELNOS ADMISSIONS ATHLETICS CAMPUSLIFE RESEARCH DOMATE			ABOUT PVAMU ACADEMICS ADMISSIONS ATHLETICS CAMPUSLIFE RESEARCH DONATE
		ETICS CAMPUS LIFE RESEARCH DONATE	Training
Resources for Telecommuting and Remote Work Information Technology resources, services, and equipment to enable the success of PVAMU Students, Faculty and Staff working remotely.			PVAMU Telecommuting Telecommuting Page Important telecommuting tools, tips, and guides can be found here. Telecommuting Page
			PVAMU Training Documentation and Resources
50	2	Ê	IMPORTANT: The online versions of all training documentation will be maintained and kept up to date on a regular basis. As a result, printed versions of documentation can be potentially outdated by the time you wish to use it. When in doubt, refer to the online version for the most recent information.
		_	Cisco IP Communicator User Guide (PDF)
For Students	For Faculty	<u>For Staff</u>	Gisco IP Communicator Phone Screen Features Quick Guide (PDF)
tal for online classes	eCourses : PVAMUs portal for online classes	DocuSign: Allows documents to be created, routed and signed with an elec	Cisco IP Communicator Interface Quick Guide (PDF)
fication	Continued Teaching Contingency Plan	DUD : Two Factor Authentication	Docusign Basic Training (Video/Demo)
IT assistance inables virtualized remote desktops and applications access for students, faculty, &	<u>DocuSign</u> : Allows documents to be created, routed and signed with an electronic signature <u>DUD</u> : Two Factor Authentication	 ITS Help Line: To request IT assistance <u>Panther Virtual Desktop</u>: Enables virtualized remote desktops and applicati 	
rage and sharing	 ITS Help Line: To request IT assistance Panther Virtual Desktop: Enables virtualized remote desktops and applications access for students, faculty, & 	staff. Syncplicity: Online file storage and sharing	DUO Instructional Guide (PDF)
is an online meeting that allows you to virtually meet with other people, without e.	staff. <u>Syncplicity:</u> Online file storage and sharing	<u>VPN</u> : To access online resources available on-campus <u>WebEx</u> : Online meeting tool	Essential Tools for Remote Working (Presentation/Video)
rencing uses high-quality video and audio and is accessible on MacOS, Windows, iOS	VPN: To access online resources available on-campus Webs: A Webex meeting is an online meeting that allows you to virtually meet with other people, without	Essential Tools for Remote Working Presentation (PDP): Slides from WebE: Essential Tools for Remote Working Presentation	Essential Tools for Remote Working (PDF)
ces. Students	leaving your home or office.	Support At-A-Glance for Staff	Panther Virtual Desktop
	 Zoom: Web-based conferencing uses high-quality video and audio and is accessible on MacOS, Windows, iOS and Android mobile devices. 	<u>Accessing Voicemail Remotely</u>	X PWAMU Remote Work Toolkit (PDP)
	Essential Tools for Remote Working Presentation (PDF): Slides from WebEx presentation Fesential Tools for Remote Working Presentation (Vitef)		Synoplicity Basic Training (Video/Demo)



TechTraining@pvamu.edu

Center for Information Technology Excellence (C.I.T.E.) Prairie View A&M University