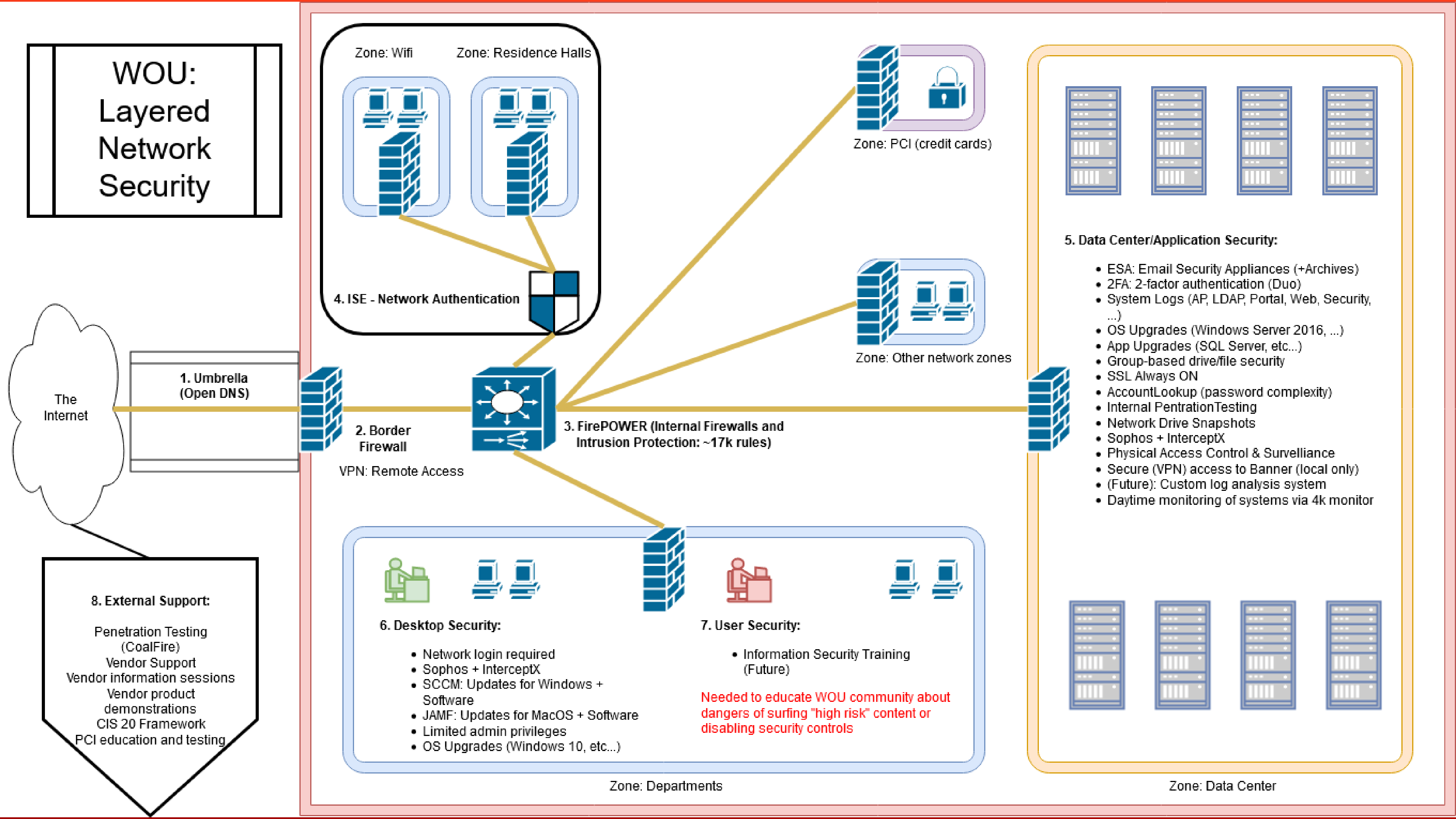
WOU CYBERSECURITY

Michael Ellis

Assistant Director, University Computing Solutions

Class of ’02 (CS), ’10 (MIS)



WOU: Layered Network Security

5. Data Center/Application Security:

- ESA: Email Security Appliances (+Archives)
- 2FA: 2-factor authentication (Duo)
- System Logs (AP, LDAP, Portal, Web, Security, ...)
- OS Upgrades (Windows Server 2016, ...)
- App Upgrades (SQL Server, etc...)
- Group-based drive/file security
- SSL Always ON
- AccountLookup (password complexity)
- Internal PentrationTesting
- Network Drive Snapshots
- Sophos + InterceptX
- Physical Access Control & Surveillance
- Secure (VPN) access to Banner (local only)
- (Future): Custom log analysis system
- Daytime monitoring of systems via 4k monitor

6. Desktop Security:

- Network login required
- Sophos + InterceptX
- SCCM: Updates for Windows + Software
- JAMF: Updates for MacOS + Software
- Limited admin privileges
- OS Upgrades (Windows 10, etc...)

7. User Security:

- Information Security Training (Future)

Needed to educate WOU community about dangers of surfing "high risk" content or disabling security controls

8. External Support:

Penetration Testing (CoalFire)
Vendor Support
Vendor information sessions
Vendor product demonstrations
CIS 20 Framework
PCI education and testing

CIS Controls™

V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

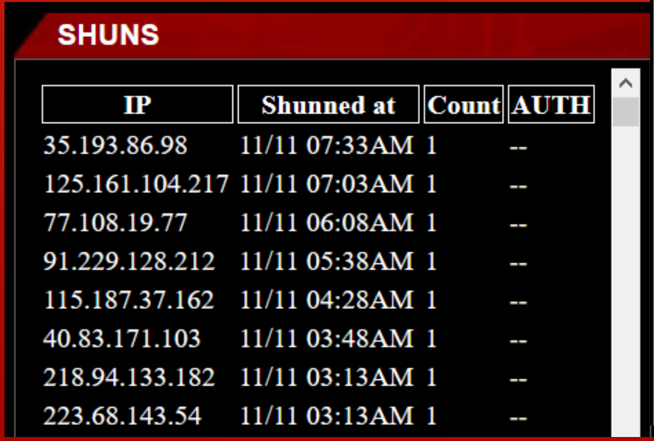
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

redWOLF^{3}

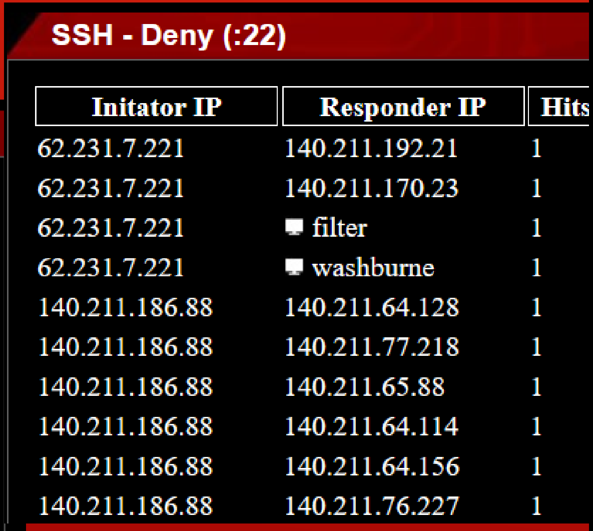
Built to meet CIS20 controls – and provide advanced analytics

- redWOLF3 is a logging, reporting and response tool
- Provides advanced analysis of firewall data and logs
- Highly customizable
- Able to create notifications, and trigger live SHUN 24/7/365
- Growing into a SIEM



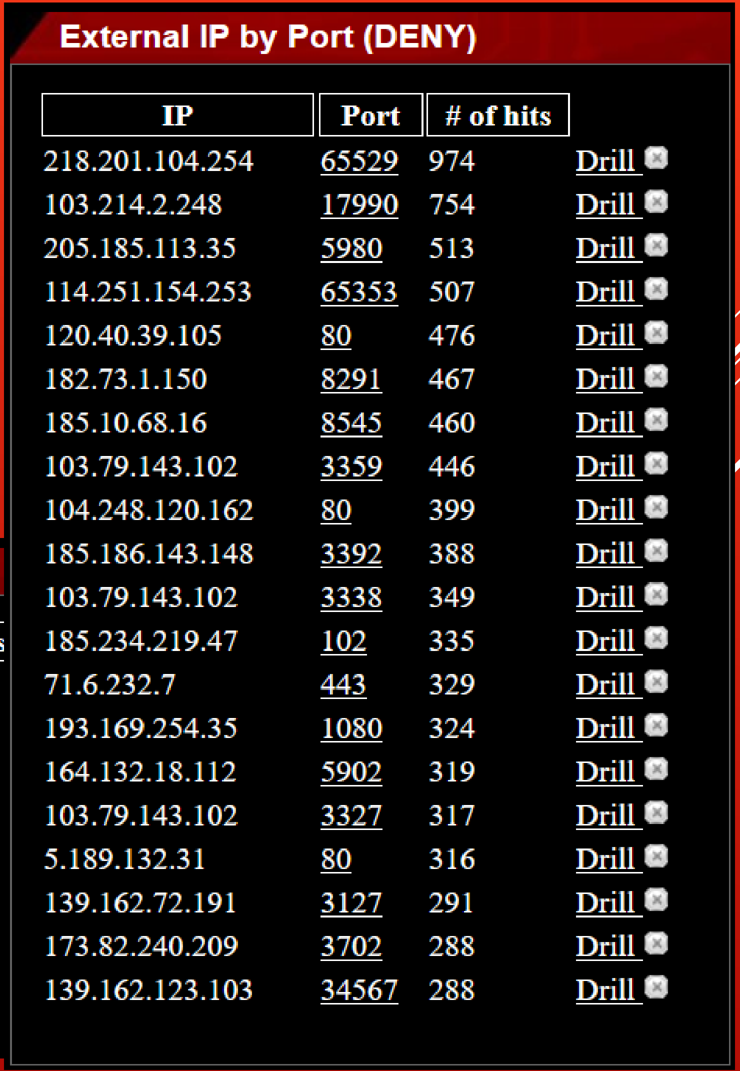
SHUNS

IP	Shunned at	Count	AUTH
35.193.86.98	11/11 07:33AM	1	--
125.161.104.217	11/11 07:03AM	1	--
77.108.19.77	11/11 06:08AM	1	--
91.229.128.212	11/11 05:38AM	1	--
115.187.37.162	11/11 04:28AM	1	--
40.83.171.103	11/11 03:48AM	1	--
218.94.133.182	11/11 03:13AM	1	--
223.68.143.54	11/11 03:13AM	1	--



SSH - Deny (:22)

Initator IP	Responder IP	Hits
62.231.7.221	140.211.192.21	1
62.231.7.221	140.211.170.23	1
62.231.7.221	filter	1
62.231.7.221	washburne	1
140.211.186.88	140.211.64.128	1
140.211.186.88	140.211.77.218	1
140.211.186.88	140.211.65.88	1
140.211.186.88	140.211.64.114	1
140.211.186.88	140.211.64.156	1
140.211.186.88	140.211.76.227	1



External IP by Port (DENY)

IP	Port	# of hits	
218.201.104.254	65529	974	Drill
103.214.2.248	17990	754	Drill
205.185.113.35	5980	513	Drill
114.251.154.253	65353	507	Drill
120.40.39.105	80	476	Drill
182.73.1.150	8291	467	Drill
185.10.68.16	8545	460	Drill
103.79.143.102	3359	446	Drill
104.248.120.162	80	399	Drill
185.186.143.148	3392	388	Drill
103.79.143.102	3338	349	Drill
185.234.219.47	102	335	Drill
71.6.232.7	443	329	Drill
193.169.254.35	1080	324	Drill
164.132.18.112	5902	319	Drill
103.79.143.102	3327	317	Drill
5.189.132.31	80	316	Drill
139.162.72.191	3127	291	Drill
173.82.240.209	3702	288	Drill
139.162.123.103	34567	288	Drill

WHAT WE ARE CURRENTLY BLOCKING

During the month of October…

- ASA (border firewall): **26.1M** (estimate)
- FirePOWER (internal firewall): **81.3M**
- SPAM: **15.8M**
- DNS/Umbrella (malicious webpage requests): **2.23M**
- redWOLF3 SHUNS: **1132** (only 47 done manually)
- Sophos antivirus: **3.3M**

Multi-year Network redesign in process! Will shrink our digital “attack surface”.

DUO STATUS

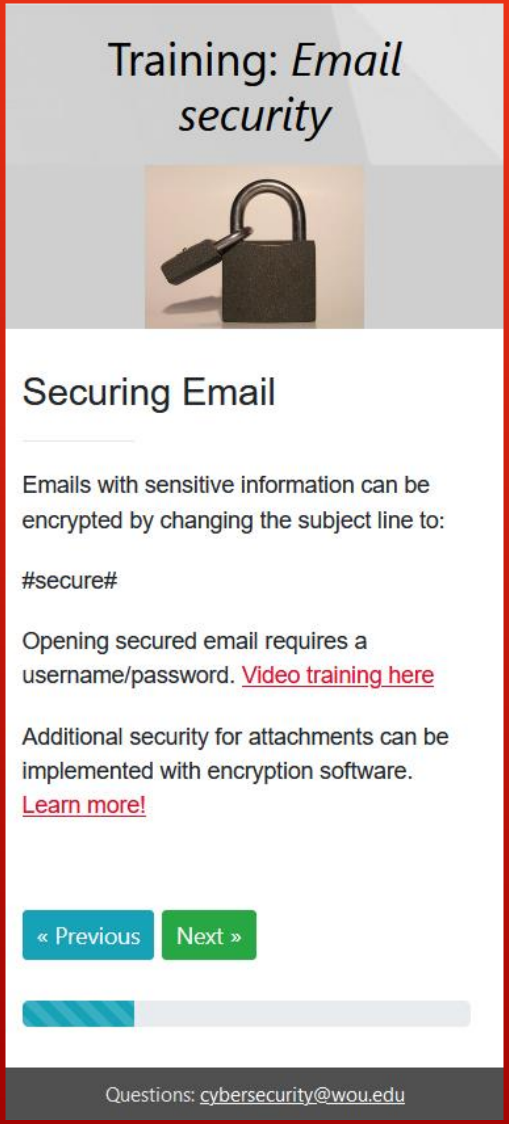
- DUO is multi-factor authentication for WOU Portal
- Met with nearly every department/division to explain DUO
- As of 11/11/19, we have 50% of our 897 Faculty/Staff enrolled in DUO
- The goal remains to have all Faculty/Staff in DUO by end-of-term
- Sending bi-monthly reports to Directors and Division Chairs with DUO enrollment status
- Discussing opening DUO to students in Winter Term

INFORMATION SECURITY TRAINING

Information Security Training Program!

- Rollout scheduled for 12/2/19
- Delivered as “bite sized” chunks (via Portal)
  - 3-5 minute lesson every 2 weeks
  - 26 lessons per year instead of a single 2hour training
  - Topics include phishing, passwords, etc…
- Available to faculty, staff and students
- Total customizability – can include timely addition of emerging threats
- Feedback built into the tool

INFORMATION SECURITY TRAINING



Training: *Email security*

Securing Email

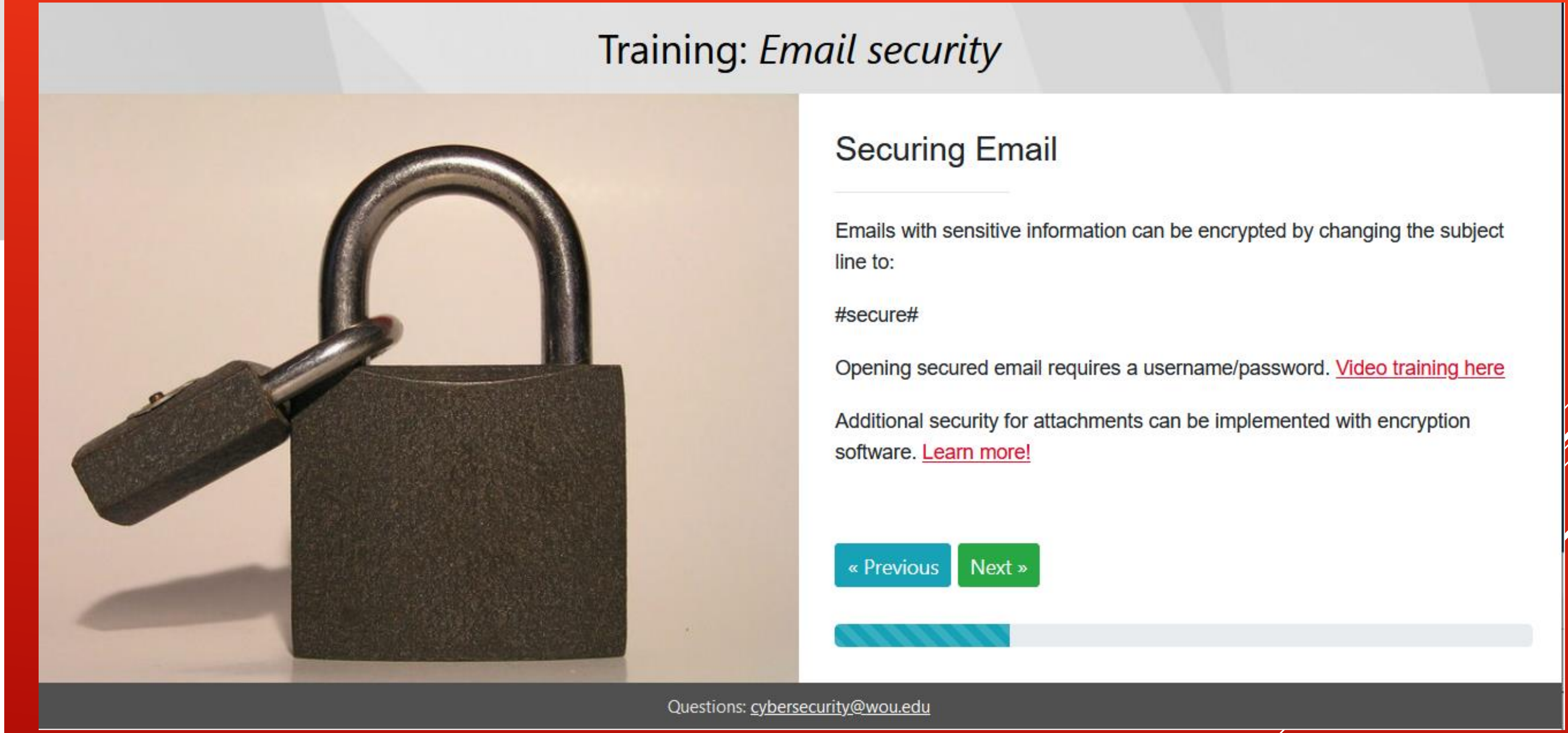
Emails with sensitive information can be encrypted by changing the subject line to:

#secure#

Opening secured email requires a username/password. Video training here

Additional security for attachments can be implemented with encryption software. Learn more!

Questions: cybersecurity@wou.edu



Training: *Email security*

Securing Email

Emails with sensitive information can be encrypted by changing the subject line to:

#secure#

Opening secured email requires a username/password. Video training here

Additional security for attachments can be implemented with encryption software. Learn more!

Questions: cybersecurity@wou.edu

QUESTIONS?