Cybersecurity Awareness

bit.ly/InfosecAware
Who am I?

Jesse Moore
Cybersecurity Advisor
UW Office of the CISO (Chief Information Security Officer) | Bothell-IT

Previously worked at:

• (4 Years) University of Washington Medicine in the Threat Detection & Response Team.

• (15 years) Nintendo of America in various roles.
Policies & Laws

UW Policy Directory

Policy Directory > APS Home

Administrative Policy Statements

Section 00—Organization, Communications, & Information Management

1.1 University Organization Chart
1.2 University-Wide Leadership List
1.3 University Government Relations and Lobbying Elected Officials
1.4 Rules Coordination
1.5 Open Public Meetings Act: Requirements to File Meeting Notices
2.2 University Privacy Policy

2.3 Information Technology, Telecommunications and Networking Projects and Acquisitions Policy
2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
2.5 Information Security and Privacy Incident Reporting and Management Policy
2.6 Information Security Controls and Operational Practices

FERPA
PCI
PHI/HIPAA
GDPR

HB 1017-2019-20
Protecting Personal Information

PDPA
Personal Data Processing Agreement

Security Terms & Conditions

UNIVERSITY of WASHINGTON | BOTHELL
Headlines 2019

Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets
University of Hawaii, University of Washington and MIT are among schools hit by cyberattacks

Sammamish Ransomware Attack: Law Enforcement Now Involved
The city of Sammamish provided an update on the ongoing ransomware attack Thursday evening.

Ransomware attack on Northshore School District Washington
25. September 2019
Northshore School District Washington was reportedly hit by a cyberattack on Friday last week i.e September 20th, 2019. Highly placed sources say that the attack was a ransomware variant which locked down access to student and staff related data. As an abundance of caution, the phone communication systems including voice mail and email servers were [...]
Types of Threats

One of everything...

- **Nation-States**: Unlimited resources to employ skilled hackers
- **Targeted Attacks**: Hacktivist for social/political ends
- **Script-Kiddies**: Looks for targets of opportunity, and have low skills
- **Insider Threats**: Disgruntled workers, contractors
The University of Washington

High Research Activity
Medical Center
ISP / K-20 provider

Office of the CISO
Security is everyone’s responsibility
Major Attack Vector: Phishing

- I want you to provide me with something.
- Typically money or access (your credentials) to systems/services

If you're not expecting it, and the email tone is demanding or makes it seem like an emergency or worse extortion for $$$ (Gift Cards: iTunes, GooglePlay, Bitcoin, etc) then be suspicious.
Major Attack Vector:

Phishing

I want you to provide me with something. Typically money or access (your credentials) to systems/services. If you're not expecting it, and the email tone is demanding or makes it seem like an emergency or worse extortion for $$$ (Gift Cards: iTunes, Google Play, Bitcoin, etc) then be suspicious.

https://ciso.uw.edu/education/scams/

Scams

Scams targeting UW students and staff

Recently there has been a surge in email, text and phone scams aimed at UW students and staff. These hoaxes are not new but they are constantly being adapted in order to better target personal and financial information and accounts belonging to members of the UW community. These scammers may:

- Ask you to buy gift cards or to send or receive money advances with the promise of easy jobs, tuition discounts or other rewards.
- Entice you with internships, financial aid or tuition payments.
- Send messages that appear to be from UW employees, but they are sent from phony or spoofed email accounts.
- Ask you to provide a cell phone number or non-UW email address in order to contact you via alternative methods.

Stay aware and protect your UW NetID credentials

https://ciso.uw.edu/education/scams/
UW NetID Credentials: Why are they a target?
Why me?
Phishing by the numbers: 2018

2,804 compromised uw net-id accounts

762 phished (27% of all compromised accounts)
What Can I Do?

> For spam and phishing, send email (with suspicious email attached) to:

EMAIL: help@uw.edu
Questions?