



35th Anniversary
National
Conference
July 18-21, 2022



Cyber Crime Raising Public Awareness

Dr. Phyllis Witt, Seduire International
Dr. Kathleen Williams, Life University
Dr. Georgianna Laws, UNT Dallas

Overview

- The devastating impact cyber crime can have on the life of a distance-learning professional who is both a researcher and a practitioner.
- What the literature reflects on the topic.
- How to stay safe.

The Impact of Infiltrated Networks

Dr. Phyllis Witt



Common Devastating Cybercrimes

Phishing

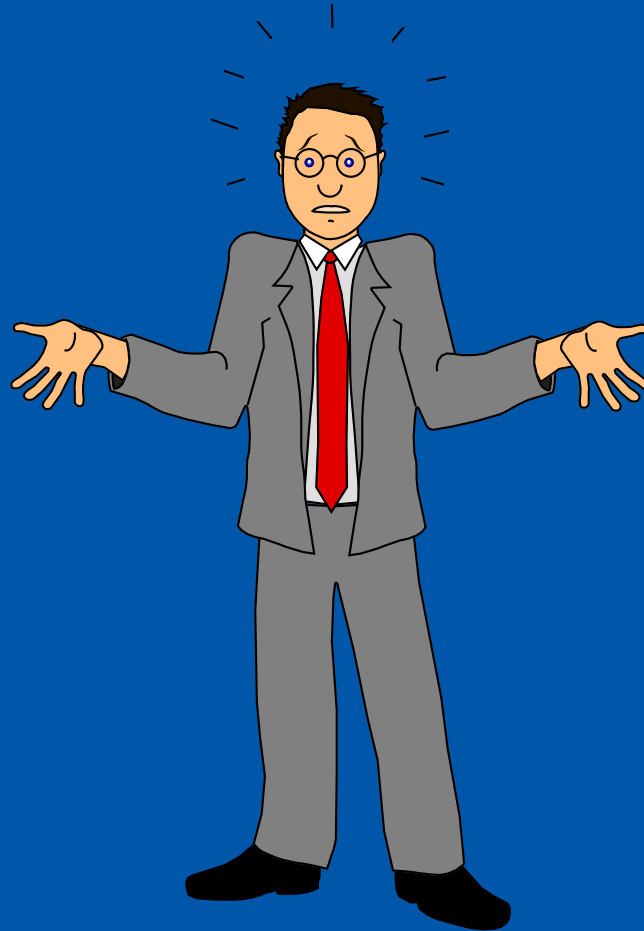
Ransomware

Identity Theft

Cyberstalking

Malware

Computer Viruses



Why is this a major concern?

The Pandemic Caused:

- A shift to remote work
- A major increase in cybercrimes

During a House Meeting in June 2020, Rep. Emanuel Cleaver Stated:

- The FBI reported seeing a 75 percent spike in cybercrimes, daily.

A Hacked Home Router

When a home router is hacked:

- All computers and devices on the network are compromised.
- All files and data are compromised.

Criminals:

- Control all computers and devices whether in on or off mode.
- Change all device and/or computer settings.
- Deny the owner access to data and apps.
- Change and block security settings.
- Restrict website access.
- Block internet access.
- Add spyware and/or malware.
- Create hidden accounts.

A Hacked Home Router

Criminals will:

- Cyber-stalk you
- Set anonymous notifications to alert the criminals each time you log on.
- Watch every site entered.
- Anonymously record and store passwords.
- Use recorded passwords for identity theft.
- Use recorded passwords to steal from bank accounts.
- Use stolen information to acquire new accounts.
- Attempt to use the cameras on all computers and devices to get a glimpse of you and your personal environment.

The Devastating Impact

You can no longer:

- Uphold privacy laws
- Secure private data (i.e., payroll, social security numbers)

Criminals can:

- Override VPNs
- Change or delete sensitive information
- Change or delete files and apps
- Enter Zoom meetings anonymously
- Write on your whiteboard during active meetings
- Change how you appear to your audience
- Do everything within their power to annoy you
- Hinder and/or hurt performance.

The Literature

Dr. Kathleen Williams



How Big of A Concern Is This?

Fortune Magazine

- 105% surge nationally in cyberattacks in 2021

Verizon Data Breach Incident Report 2022

- Frequency: 1,241 incidents, 282 with confirmed data disclosure
- Motives: Financial (95%), Espionage (5%)

Cyber attacks on educational institutions are quickly growing

Post-COVID Attacks

- **Malware hidden in textbooks and documents**
- Hacking remote learning sessions (Zoombombing)
- Ransomware
- Phishing emails

Impacts

- Lack of access to systems can impact enrollment
- Data leaks can lead to identity theft (students and faculty)
- Infection of back-ups
- Psychological and emotional damage
- Increase in premiums for cybersecurity insurance
- Cyberpandemics

How Does This Happen?

- Non-deletion of accounts after resignation or job change
- Lack of or infrequent access control audits
- Shortage of people working in cybersecurity
- Threats from internal employees
- Lack of cyber safety training for staff
- Large scale growth of customer facing networks and online cloud technologies
- Unsecure home networks (Remote work)

Cyberhygiene

Dr. Georgianna Laws



It's on Us

- How do you keep your home safe when you go on vacation?
 - Neighborhood police patrol
 - Security system
 - Cameras
- Do you lock your doors/windows?
- Do you give anyone the key to your home?

Passwords

Characteristics

- Numbers
- Letters (Upper & Lowercase)
- Special Characters
- Phrases
- Two-factor authentication

Frequency of Change

- Every Semester

Storage – Pros and Cons

- Written
- Password Vault
- Memorized

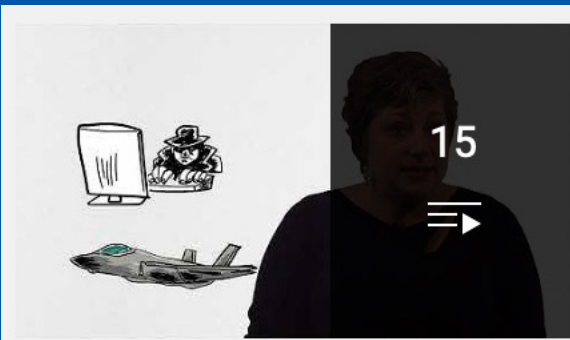
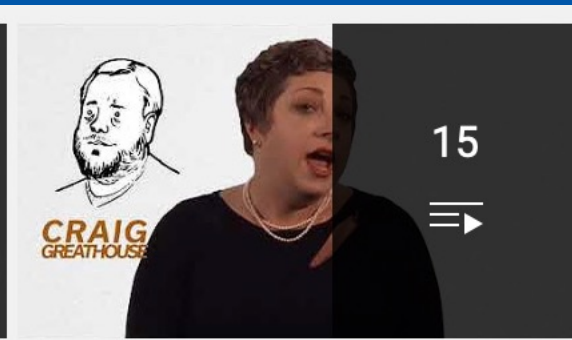
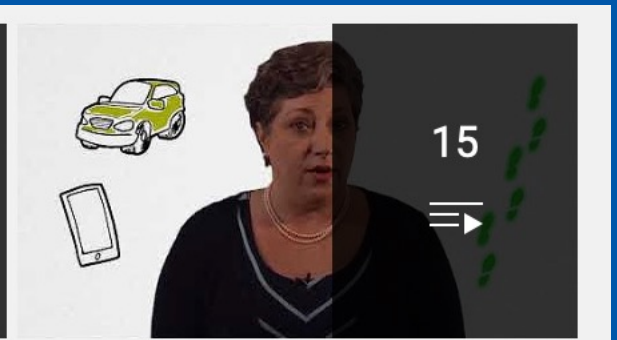


Staying Safe at Work

Preventative Methods

- Training
- Look out for anything “phishy”
- Lock your computer when you step away
- Have a strong, unique password that you change frequently, etc.

Free Cybersecurity Classes

 <p>15</p>	 <p>15</p>	 <p>15</p>
<p>The Global Cyber Threat Environment</p> <p>VIEW FULL PLAYLIST</p>	<p>Cyber Conflict</p> <p>VIEW FULL PLAYLIST</p>	<p>Strategic Cybersecurity</p> <p>VIEW FULL PLAYLIST</p>



Staying Safe at Home

Identity Security

- Careful with whom you share your SSN

Device Security

- Device password
- Admin account

Home Network Security

- Change the default internet password
- Encrypt your internet

Think Before You Share

- **Social engineers** get people to do what they are not supposed to do.
- Hackers can leverage what you share in order to engineer a targeted attack you are likely to fall for
- Limit personal information you share on social media
 - Checking in
 - Favorite things
 - Providers you use, etc.

Think Before You Click

Look for warning signs

Sender

- Public domain email address
 - e.g., email from PayPal coming from a Gmail account
- Domain name misspelled

Message

- Poorly written
- May refer to something you know well/use
- Asks you to click, download, authenticate, etc.
- Creates a sense of urgency

Learn from the world's most famous hacker, Kevin Mitnick

- <https://www.mitnicksecurity.com>

Think Ahead

Use Virtual Private Network (VPN)

- <https://www.pcmag.com/picks/the-best-free-vpns>

Avoid free, unencrypted wi-fi connections

Back up your important data

- Cloud
- External disk
- Ransomware proof

Use an RFID wallet when you travel, etc.

Q&A, Contact, and Handout

Dr. Phyllis Witt

Dr.phyl.edd@protonmail.com

Dr. Kathleen Williams

kewillia6@gmail.com

Dr. Georgianna Laws

drglaws@gmail.com



SCAN ME