I. Introduction

A. Format of the class

1. Interactive

II. Check your Coordinates

A. Secure connections and domain names

1. The padlock and HTTPS

2. Certificates and benign errors

B. Tool tip reveals

1. Hover over the link to see where it leads

C. Browser warnings

1. Sometimes a pain, sometimes worth a second look

III. Mobile Device Mayhem

A. Phishing text messages

1. Telltale signs; what to do

B. Telemarketers

1. Don't give them an inch.

C. Recordings

1. If they don't have the time to talk to you in person, you don't have the time either.

IV. Email Errors

A. Spoofing and phishing scams

1. Your best friend probably isn't a Nigerian prince, and he doesn't know he sent you that email.

B. Better log in manually than use a link

1. It says it's your bank. Don't click the link; log in manually, on your own.

C. Beware panic-inducing messages

1. Panic short-circuits logiThat's why it's so effective.

D. Don't give out your logins

1. 99.9999% of the time, legitimate businesses don't need your logins.

V. Workplace Woes

A. Audit trails and shared logins

1. Most company software tracks what everyone did and when

2. Don't let your coworker use your login, and refuse to use shared logins

B. Borrow my badge

1. Physical security prevention prevents cyber security ailments

C. Assume everything is recorded

1. Keystroke loggers and screenshot software

- D. Copiers have memories
  - 1. Don't make copies of credit cards, passports, driver's licenses, etc.
- E. Don't give customers your cell number
  - 1. Keep boundaries; you don't need strangers calling you at home

VI. Public Wifi Purgatory
- A. VPNs
  - 1. Not as hard as it sounds
- B. No sensitive info
  - 1. Public wifi is easy to hack
- C. Background data
  - 1. Your device isn't really asleep
  - 2. Info can be flowing without you knowing
  - 3. If you have to surf at Starbucks, keep it quick

VII. Insurance
- A. Separate or bundled
  - 1. Antivirus companies sometimes offer multiple plans
- B. Shop around
  - 1. There are many different kinds, and your employer or ISP might offer something

VIII. Apetite for Antivirus
- A. Someone's gotta be first
  - 1. Zero-day exploits and why you need protection - it's in the news? Great! You're already infected.
- B. Root kits and ransomware
  - 1. Steps toward mitigating the risk

VIII. I Beg you to Back Up
- A. So many options; pick at least two
  - 1. USB hard drives; NAS; backup services, online storage through the office suite
- B. Rotation routines
  - 1. The further back your backup, the more you could lose
- C. When the cloud is not enough
  - 1. Simple document sync can be problematic

IX. Password Perfection
- A. What is a strong password?
  - 1. Options for keeping them easier to remember
- B. How do I keep track of them all?
- C. When is a PIN okay to use, and what kind?