Wespath
BENEFITS | INVESTMENTS

Information Technology Security

Conference Forum | April 2023

IT Security Is Complex

Let’s Simplify—Top Cyber Threats

Social Engineering
Attackers create social situations that encourage you to share your password.

Password Attack
Attackers use various methods to break a username or discover a password.

SQL Injection
Hacker injects harmful information into an SQL statement with a security vulnerability.

Eavesdropping
Hackers monitor the platform’s traffic and ‘job.’

Denial of Service (DDoS)
An intrusion that removes links to machine services by inserting malicious traffic into the database.

Malware Attack
A malicious program that disrupts or damages the computer.

Phishing
Intruder sends bait—often as an email. Phishing invites users to communicate their information to the intruder.

IT Security Activities Underway at Wespath

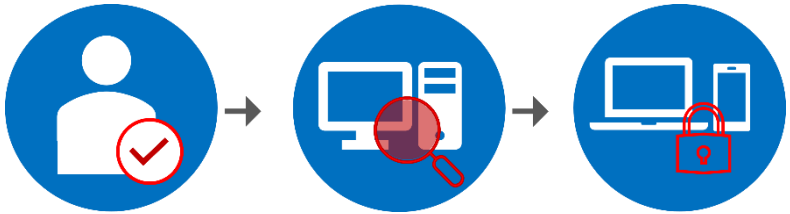
- Upgrading our endpoints (desktops, laptops, phones, etc.)
- Moving to “zero trust security”—
  we trust no one, even in our own building
- Multifactor authentication everywhere
- Very complex passwords with regular expiration
  - 16 characters, upper-/lowercase, number and special characters
- Guest WiFi isolated and secured
- Upgrading our Data Loss Prevention (DLP) tools

Zero Trust Concept

Castle and Moat

- Once you get into our network (i.e., past our moat) we implicitly trust you
- We verify your credentials and let you in the door. Some systems and records require only credential validation

Zero Trust



VERIFY THE USER | **VALIDATE THE DEVICE** | **LIMIT ACCESS AND PRIVILEGE**

- We eliminate implicit trust—everyone and their device is “guilty until proven innocent”
- Verify the person, device, type of access and location
- More multifactor authentication, just-in-time and just-enough-access, and policy-based validations
- A bevy of tools working together to improve security

Cloud Asset Sharing and Access

- Just because it's in the cloud doesn't mean it is inherently secure—**you must take ownership of security**
- Example: OneDrive's default settings give anyone with the link to an asset the ability to edit that asset
  - **Wespath has disabled this**
- **Educate your staff and yourself**
- Cloud products are very functionally rich—but makes them challenging to implement
- **Consider external help** to ensure you and your organization are safe and protected

Actions You Can Take

	Create a cadence of regular system updates (phones, endpoints, software, etc.)
	Use multifactor authentication everywhere
	Implement very complex passwords—16 characters, upper-/lowercase, numbers and special characters. Phrases work best!
	Use complex guest WiFi password—change it monthly. Phrases work best!
	Don’t broadcast WiFi name
	Educate, educate, educate your staff about phishing
	Protect your endpoints

Questions

Wespath

BENEFITS | INVESTMENTS