Information Security Awareness Training

Fall 2019

Evangelical Lutheran Church in America
God's work. Our hands.

What is Information Security?

The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Confidentiality	Integrity	Availability
Ensures that only the people who are authorized to have access to information are able to do so	Ensures that the value and the state of information are maintained (i.e., it is protected from unauthorized modification)	Ensures that information and information systems are available and operational when they are needed to support critical business processing

Why worry about security?

- You click on a web link in an unknown email allowing a virus to attack systems leaving the company unable to respond to clients and issue invoices for a month
- You accidently send out payment information to the wrong email recipient – the client would loose trust and send business elsewhere
- You are traveling in an airport and have your computer stolen and hackers gain access to all systems stealing a vast amounts of employee and client data
- You provide your user name and password to a co-worker to perform some temporary work in the systems and they maliciously extract the entire database of information – you are liable since it is your user name and password

82% of organizations have experienced a phishing attack in the past year

59% of organizations consider ransomware to be their biggest threat

It took 1 in 5 organizations between two weeks and a year to fully recover from cyber attacks

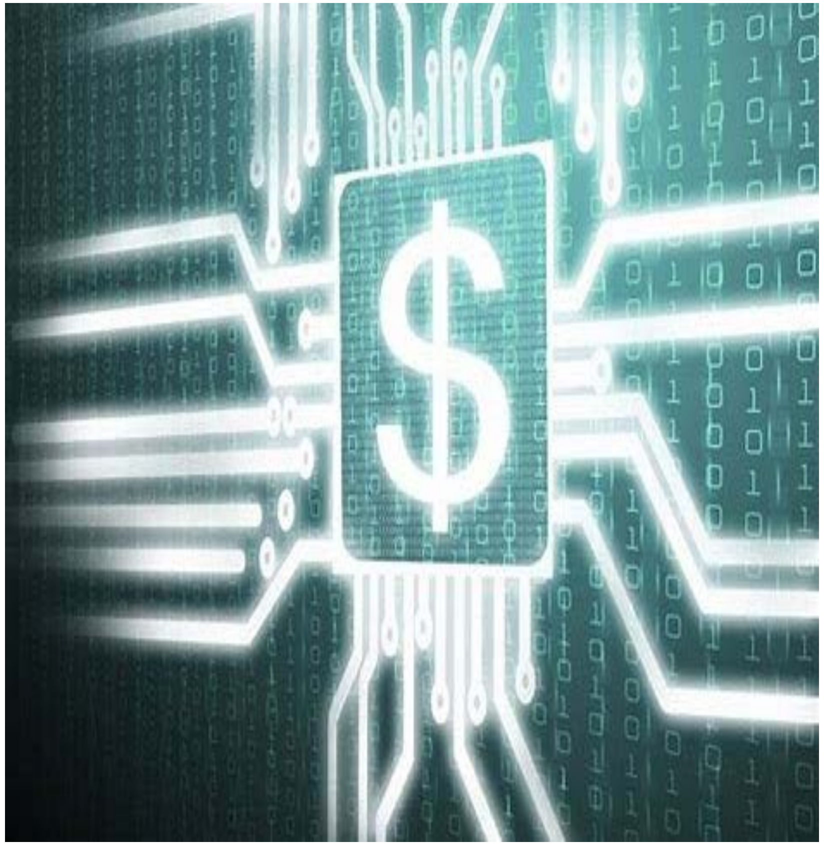
What does it cost the organization?

The global average cost of a data breach is up 6.4% over the previous year to $3.86 million

The average cost for each lost or stolen record containing sensitive and confidential information increased by 4.8% to $148

WannaCry Ransomware alone is estimated to have infected 300,000 computers around the world and have caused financial and economic losses of up to $4 billion

Cost include business disruption, revenue loss, equipment damages, legal fees, public relations expenses and forensic analysis, as well as legally mandated notification costs



Stop That Malware!

What is Malware?

Malware is software that infects computers to perform malicious actions such as gain control over your computer or devices

What is the Danger?

- Steal your User ID and Passwords
- Spy on your online activities
- Modify or delete all of your files
- Take control of your computer or files demanding that you pay a ransom to get them back
- Transmits information to unknown Internet site or remote user

Defend Your Computer

- Logoff or turn on the password-protected screensaver when you leave
- Do not click on links from suspicious emails or pop-up windows
- Ensure Antivirus software is enabled and definitions are up to date
- Keep all Microsoft Windows, Office and other software current – let the updates run
- Do not use USB Flash Drives which can introduce viruses and be easily lost

A single Antivirus product blocked 38 billion threats during the first half of 2017

Protect Sensitive Information

- Ensure web site has “https” in front of web address
- Use secure email encryption for confidential emails and documents
- Store your data on organization file servers or back up your PC data regularly
- Clear your desk at the end of the day
- Retrieve documents from printer immediately
- Dispose of sensitive documents properly in to shred bins
- Never discuss confidential information in public areas or with individuals who don’t have a need to know
- Be aware of surroundings and unauthorized overlooking (shoulder surfing)

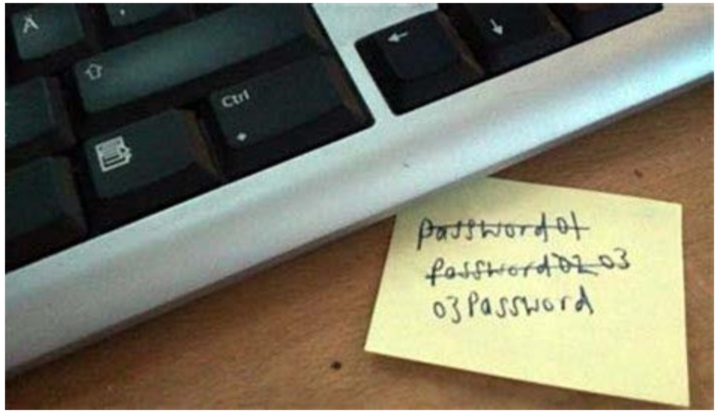
80% of security issues are caused by bad passwords

Evangelical Lutheran Church in America
God’s work. Our hands.

Create Strong Passwords and Keep Secret

- Create passwords that are made up of long phrases that mixes characters such as GPS!sth$BestC0pany$ver
- Do not use names, personal information, dictionary words, or guessable phrases
- Use different passwords for different systems and web sites
- Do not write down passwords and leave in desk drawer or on your computer
- Never share your logon ID or passwords

80% of security issues are caused by bad passwords



Evangelical Lutheran Church in America
God's work. Our hands.

Use Email Appropriately

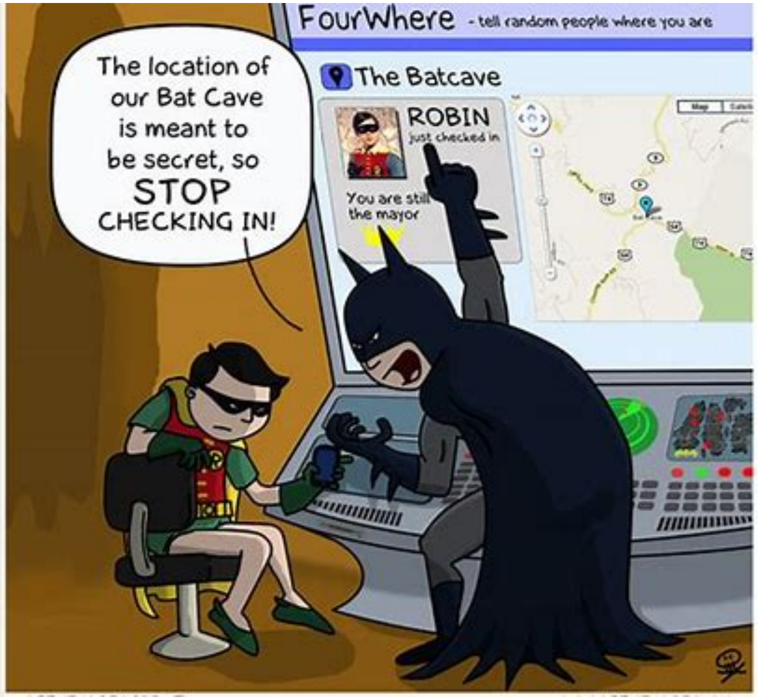
- Do not use organization email for personal use and vice versa
- Do not use organization email for the dissemination of inappropriate or offensive information
- Do use separate email accounts or addresses for different aspects of your life such as business, personal, school, sports, etc.
- Do not auto-forward messages from organization e-mail systems to personal email accounts
- Do encrypt the email or files if sending highly sensitive data
- There should be no expectation of privacy as all email can be monitored

Use the Internet Appropriately

- Accessing the Internet and web sites should only to be used for organization purposes
- Personal use of the Internet should be kept to a minimum and limited to non-working time
- Refrain from downloading copyrighted material without prior explicit written permission
- Information pertaining to the organization should never be placed on the Internet without prior approval
- Set browser security level to medium or higher to protect from malicious web sites
- There should be no expectation of privacy as it can be monitored

Use Caution on Social Media

- Do not post confidential organization or constituent details on LinkedIn, Facebook, Twitter, etc.
- Do not post or “check in” your location, especially that you are on vacation away from work or from your home
- Do not use information you put on your social media that you would use in your security questions for web accounts
- Be selective of who you connect with on social media


FourWhere - tell random people where you are
The Batcave
ROBIN
just checked in
You are still the mayor
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!

What is a Security Incident?

A “Security Incident” is any activity that has caused or may cause a breach of either physical or network security on any part of the company network

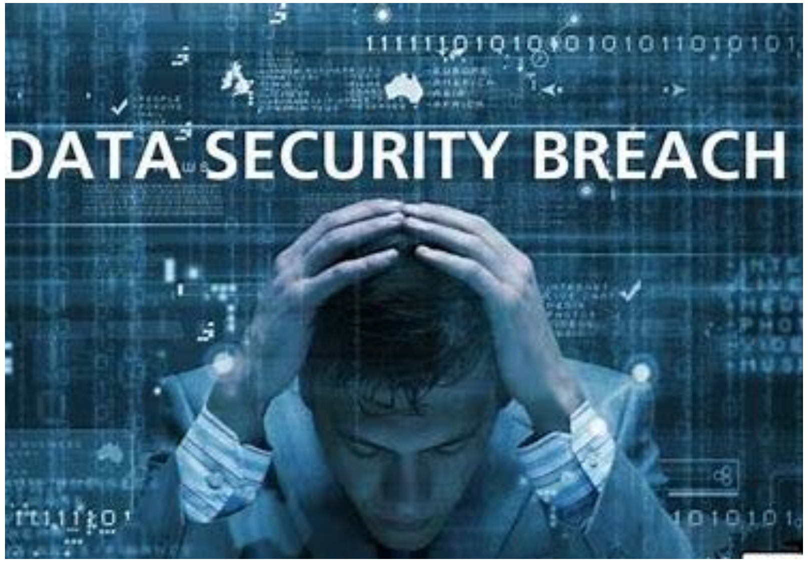
Examples of security incidents

- Unauthorized access to a system (internal or external)
- Denial of system resources
- Malicious use of system resources
- Loss, theft, or damage to a system
- Compromise of system integrity
- Discovery of fraud, inappropriate use (personal business use), and offensive or pornographic material
- Worm or virus attack

Information Security is EVERYONE’s responsibility!

You Have Been Breached, Now What?

- Immediately stop working and disconnect your computer from the network
- Document what you were doing at the time of the breach
- Contact your manager and technical support
- Follow all of the directions you receive



Report Policy Violations and Security Incidents

- As an employee of the organization, you have an obligation to report any known or suspected abuse, misuse or theft of the organization's data, equipment or electronic information systems
- Immediately report violation or incident to technical support, your supervisor, and/or human resources
- Further investigation, review or corrective action will be conducted and forward to appropriate management for final review
- Any criminal activity will be forwarded immediately to the appropriate law enforcement agency
- Any breach of confidential information will be communicated by appropriate management

Questions?

Evangelical Lutheran Church in America
God's work. Our hands.