Information Security Webinar

April 21, 2020

Chris Hueneke
Chief Information Security Officer at RKON
Information Security Advisor for the ELCA
CISSP, ISO 27001 Auditor, ITIL

Member of Bethany Lutheran Church, Lemont, IL

Chris Hueneke, Chief Information Security Officer at RKON, is an IT security leader with over 25 years of experience in the industry. His professional experience includes advising and implementing global IT governance, risk, compliance, and security control frameworks and solutions. He has diverse IT risk and security experience protecting international organizations throughout the world for industries such as private equity, financial services, retail, manufacturing, and airlines. Chris' extensive global leadership experience includes building IT risk and security teams from the ground up and consulting on improvements in endpoint, perimeter, datacenter, and cloud security architectures. He is a visionary leader able to communicate technology strategy, compliance, architecture, and critical risks effectively to key stakeholders, executive leadership, and boards of directors

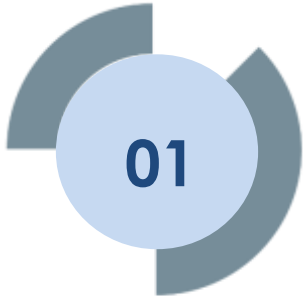
Shark Tank Host Loses $400k in Email Scam

New York (CNN Business) – "Shark Tank" judge Barbara Corcoran lost nearly $400,000 in an elaborate email scam that tricked her staff.

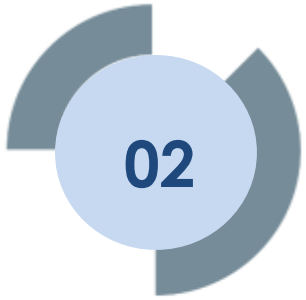
Corcoran said someone acting as her assistant sent an invoice to her bookkeeper earlier this week for a renovation payment. She told People that she had "no reason to be suspicious" about the email because she invest in real estate, so the bookkeeper wired $388,700 to the email address.

- Hackers used publicly available information and email scam to pose as a credible source and tricked her organization into wiring money - she was not hacked into
- Hackers used "Whaling" techniques to target the executive - "Shark Tank Judge got Whaled"
- Barbara Corcoran may not be in the Non-Profit arena, but nevertheless she fell victim to the exact same process that is being used to target other organizations including church organizations

Webinar Agenda



Information Security Overview



Primary Attack Methods

User Role in Preventing Attacks

Cyber Security Incident Reporting

Information Security Overview

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 cyber security?

1. You send out thousands of dollars in a wire transfer to a criminal
2. You click on a web link that locks your computer
3. Your computer is stolen at an airport
4. You provide your password to a disgruntled employee
5. You download free software from the Internet

86% of organizations faced a phishing attack in the past year

59% of organizations consider ransomware to be their biggest threat

47% increase in number of insider-driven data breaches

Proofpoint - 2020 State of the Phish

What does cyber security attacks cost the organization?

- 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
- The average cost for each lost or stolen record containing sensitive and confidential information increased by 4.8% to $148
- The global average cost of a data breach is up 6.4% over the previous year to $3.86 million
- Cost include business disruption, revenue loss, equipment damages, legal fees, public relations expenses and forensic analysis, as well as legally mandated notification costs

Primary Attack Methods

Top 5 Cybersecurity Threats

1. **Malware** - Automated method into an organization for hackers to disrupt, damage, or gain unauthorized access to a computer system
2. **Ransomware** – Malware typically distributed through spam email attacks that blocks access to critical business data
3. **Phishing** – Email impersonation or spoofing to obtain sensitive information such as usernames, passwords and credit card details, generally leading to attempting to commit financial fraud
4. **Social Engineering** – Manipulating individuals via email, phone, or networks into divulging confidential or personal information to be used for fraudulent purposes
5. **Misconfiguration** – Attackers taking advantage of security architecture design flaws and misconfiguration of security controls

Can You Trust that Web Link or Attachment?

Malware: Targeting Computers

Attackers creating and delivering software that infects computers to perform malicious actions such as gain control over your computer, mobile devices, printers, scanners, etc.

What is the Danger?

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

Can You Trust that Email Message?

Phishing: Targeting Mass Audience

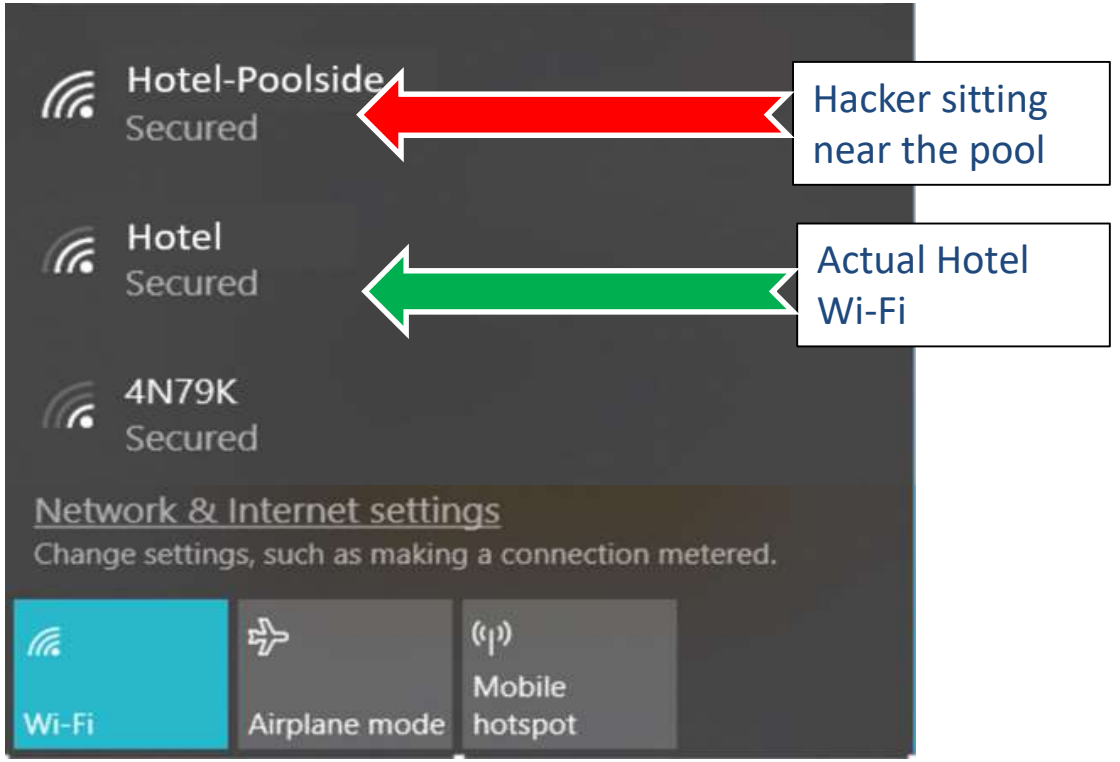
Attackers sending emails impersonating reputable parties in order to induce many employees to reveal personal information, such as passwords and credit card numbers

Whaling: Targeting Specific High Value Targets

Attackers spear phishing a specific high value target such as an individual executive or leader, usually spoofing email as a precursor to wire fraud

Can You Trust the Public WiFi Network?

<u>Social Engineering:</u> The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes



- Hackers can sit quietly with their laptops nearby and create look-alike Wi-Fi networks
- Ask hotel or coffee shop for the exact name of the Wi-Fi networks

Can You Trust the Software?

For example, Zoom is being utilized as a virtual gathering tool for many working from home

- ZoomBombing is an invasion of unwanted attendees
- Flaw with configuration of Zoom waiting rooms
- Accounts found on the dark web
- Sharing personal data with advertisers

User Role in Preventing Attacks

Defend Your Computer

- ✓ Logoff or turn on the password-protected screensaver when you leave your computer
- ✓ 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 operating systems, applications, and mobile devices 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 **ALL** Sensitive Information

Electronic Information

- ✓ Ensure web site has "https" in front of web address
- ✓ Use encryption to secure confidential emails and documents
- ✓ Store your data on organization file servers or back up your PC data regularly

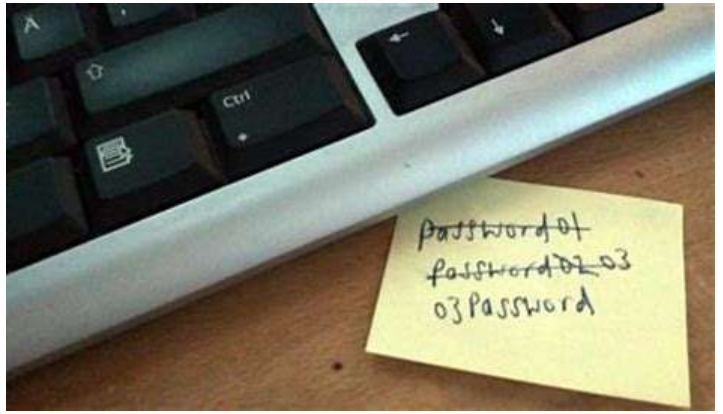
Physical Information

- ✓ Clear your desk of any sensitive documents and lock in a cabinet
- ✓ Retrieve documents from printer immediately
- ✓ Dispose of sensitive documents properly in a shredder or 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)

Create Strong Passwords and Keep Secret

- ✓ Create passwords that are made up of long phrases that mixes characters such as ELCA!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 with anyone

80% of security issues are caused by bad passwords



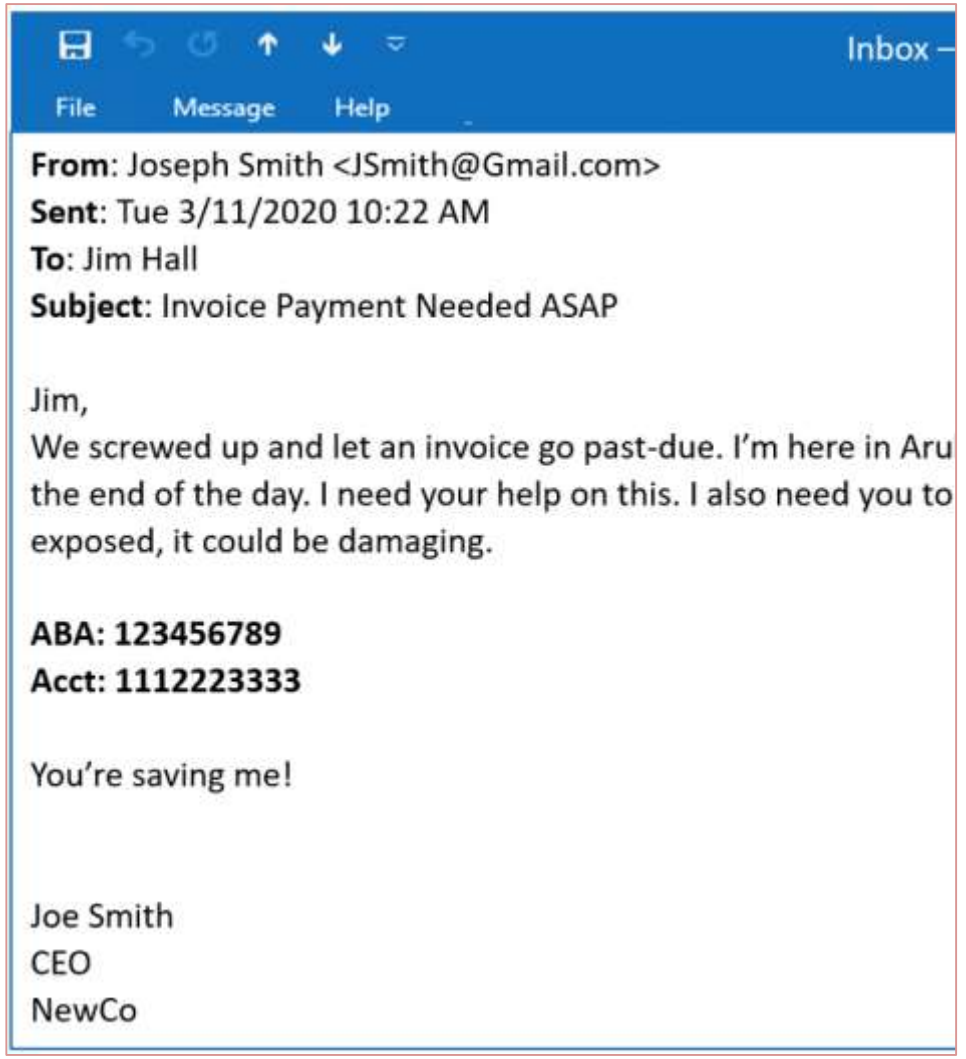
Use Email Appropriately

- ✓ Do not use organization email for personal use and vice versa
- ✓ 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
- ✓ Do not use organization email for the dissemination of inappropriate or offensive information
- ✓ There should be no expectation of privacy as all email can be monitored

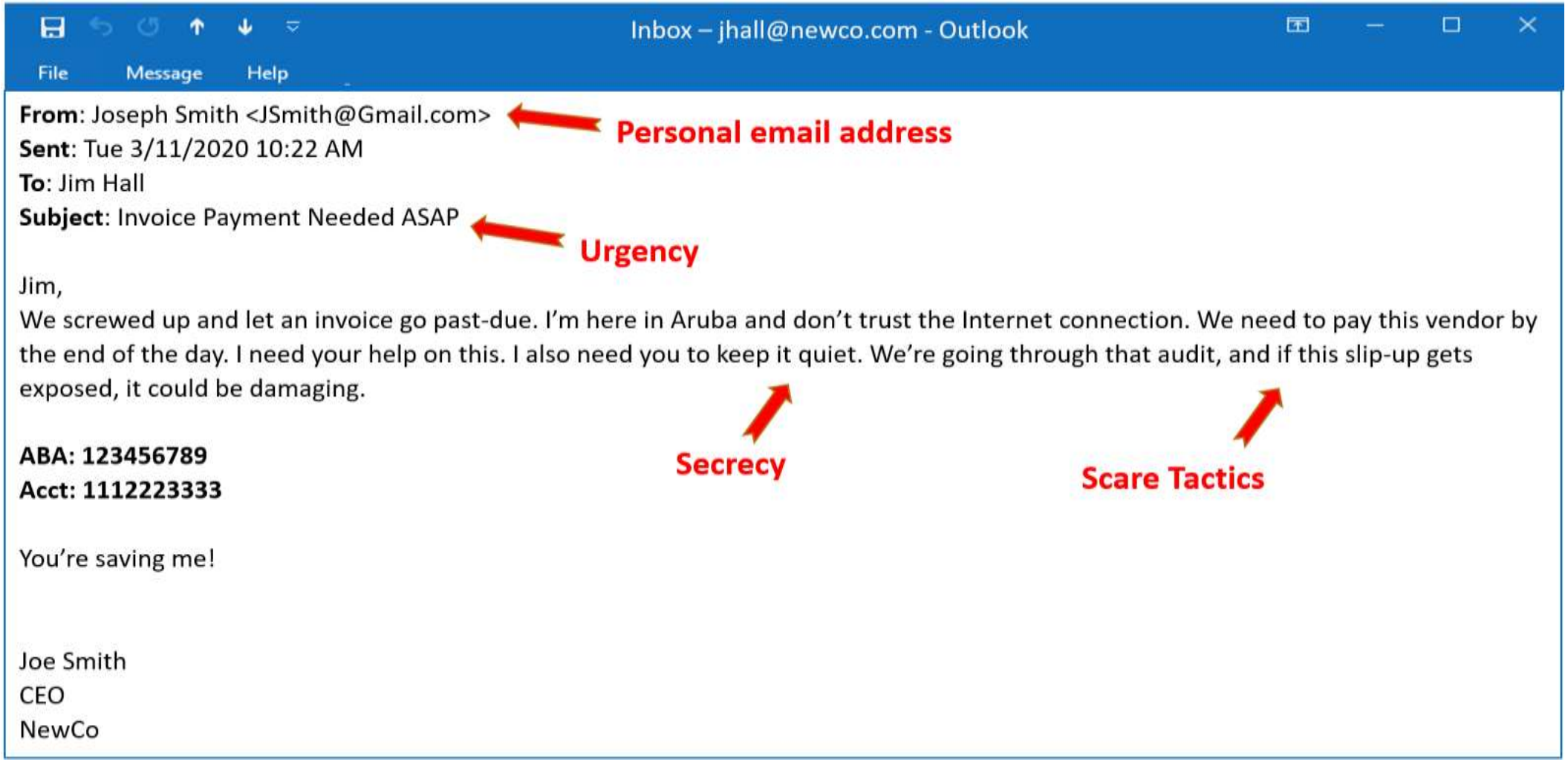
FBI reported $1.7 Billion stolen in 2019 by email spoofing, or Business Email Compromise

Avoid Phishing Emails

- ✓ Does it contain a link?
- ✓ Does it contain an attachment?
- ✓ Does it ask for money, credentials, or sensitive info?
- ✓ Do you know who it's from?
- ✓ Can you verify who sent it?
- ✓ Are you really sure?



Email Impersonation Signs



Who Really Sent that Email?

- ✓ JSmith@NewC0.com **That's a Zero!**
- ✓ Jsmith@Gmail.com **That's Gmail account!**
- ✓ Jsmith@NewCo.com **That's perfect! Uh-oh.**

Bottom line, you cannot trust the "From:" address

- Savvy attackers can directly manipulate the "From:" address
- Recipient unable to spot the discrepancy
- Sender unaware their password has been stolen
- Lack of email authentication protocol adoption

Avoid Phone Call Scams

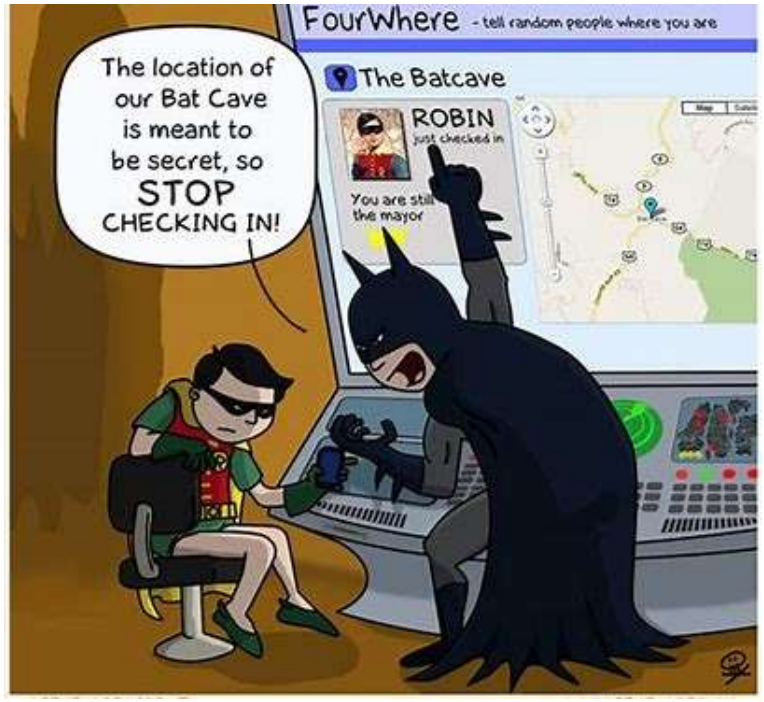
- ✓ Be extremely suspicious if someone creates a sense of urgency, putting pressure on you to do something
- ✓ Confirm the caller's identity with a PIN or established security questions
- ✓ If you believe a phone call is an attack, simply hang up and contact the organization by looking up on their website
- ✓ Never allow a caller to take temporary control of your computer or trick you into downloading software

Use the Internet Appropriately

- ✓ Set browser security level to medium or higher to protect from malicious web sites
- ✓ 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
- ✓ Information pertaining to the organization should never be placed on the Internet without prior approval
- ✓ Refrain from downloading copyrighted material without prior explicit written permission
- ✓ 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



Do's and Don'ts to Prevent Attacks

	CYBER ATTACK PREVENTION CHECKLIST
✓	Ensure you have security solutions implemented and working properly such as firewalls, anti-virus, advanced email security, and multi-factor authentication
✓	Limit number of people who are authorized to complete financial transfers – establish internal department rules to follow up with phone call and don't just rely on email
✓	Be cautious of personal Email addresses – only use company email
✓	Never give your password to personnel from the help desk or IT – use password self-service reset
✓	Be cautious when clicking on links and downloading attachments in email – delete suspicious email
✓	Don't follow links in email requesting to change passwords - visit the website by typing the address yourself
✓	Don't post company information or vacation schedules on social media – keep confidential
✓	Don't insert unknown USB thumb drives into any computer – report found USB drives to IT Security
✓	Be aware of the criminal presence and malicious wireless networks in public spaces – use mobile hotspot or Virtual Private network on known networks

Cyber Security Incident Reporting

What is a Security Incident?

A "Security Incident" is any activity that has caused or may cause a breach of physical or technical security

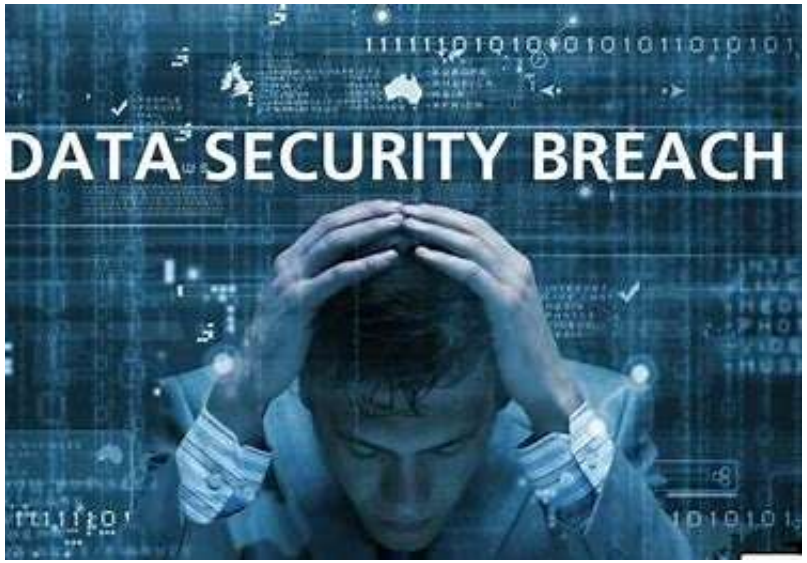
Examples of security incidents

- Worm or virus attack
- 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

Information Security is EVERYONE's responsibility!

You Have Been Breached, Now What?

1. Immediately stop working and disconnect your computer from the network
2. Report the breach to your supervisor or leadership and technical support
3. Document what you were doing at the time of the breach
4. Follow all of the directions you receive from leadership and IT



Security Incident Handling Guidelines

- Employees of the organization should have an obligation to report any known or suspected abuse, misuse or theft of the organization's data, equipment or electronic information systems
- Violations or incidents should be reported to technical support, supervisor, and/or human resources
- Investigation or corrective action should be conducted and forwarded to appropriate leadership for final review
- Any criminal activity should be forwarded immediately to the appropriate law enforcement agency
- Any breach of confidential information should be communicated by appropriate leadership
- If the security incident impacts others or assistance is needed, leaders should contact the ELCA Churchwide Ministries or Synod for proper guidance and support

Contacts for More Information

Jonathan Beyer

Executive for Information Technology

Jonathan.Beyer@elca.org

Chris Hueneke

Information Security Advisor

Chris.Hueneke@elca.org

ELCA Information Technology Help Desk

HelpDesk@elca.org

ELCA Information Technology Training

TechTraining@elca.org

Mission Investment Fund Red Flag Compliance

What is Red Flag Compliance?

- The "Red Flag Rule" was created by the Federal Trade Commission and other government agencies to help protect customer data and Personal Identity Information (PII) and prevent identity theft
- A "Red Flag" is a pattern, practice, or specific activity that indicates the possible risk of identity theft

PII Types	IT Risks	IT Controls
Name & Address	Web Applications	Policies and Procedures
Birth Date	Mobile Applications	Endpoint Security
Social Security Number	Email	Perimeter Security
Credit Card	Instant Messaging	Datacenter Security
Financial	Portable Storage Devices	Cloud Security
Account and Routing Numbers	Paper Documents	Vulnerability Assessment
	Archives	Log Management
	Human Beings	Incident Response

Red Flag Do's and Don'ts

Do's

1. Identity and classify PII data
2. Inform manager of intentions to download or email PII data and obtain permission
3. Eliminate all electronic PII when no longer needed
4. Ensure all paper documents containing PII are locked or shredded when no longer needed

Don'ts

1. Download or email PII unless it is absolutely necessary for the task at hand
2. Disable password protection on desktop, web browser or files
3. Send or storage PII in email without password protection and encryption
4. Print anything containing PII unless absolutely necessary

Store all PII on MIF I:Drive, NOT on OneDrive