DANNIBLE & MCKEE, LLP

Certified Public Accountants and Consultants

Delivering **Confidence**

Don't Get Scammed, Get Educated:
How Fraudsters Attack & How You Can Protect Your Organization

Presented by:
Kaitlyn H. Axenfeld, CPA/CFF, CFE
Christine N. Petrone, CPB

January 17, 2024

Types of Fraud

- **Internal Fraud** (also known as occupational fraud) - fraud committed by people who legitimately work for or do business with a company

- **External Fraud** – fraud committed by outsiders with no legitimate business with the company

Managing Third-Party Fraud Risks

- All external parties that conduct legitimate business with an organization can pose unintentional fraud risks to the organization.

Types of Third-Party Fraud Risk:

- Legal Risk
- Ethical Risk
- Financial Risk
- Cyber Risk

Managing Third-Party Fraud Risks

Cyber Risk

A weak cybersecurity posture:

- Can make log-in and password credentials visible or easy to acquire;
- Creates a gateway for fraudsters to damage your systems via third-party system connectivity and access;
- Gives fraudsters visibility to your proprietary and confidential information that resides on the third-party system; and
- Enables fraudsters to more effectively create socially engineered phishing, smishing, and vishing communications, increasing the likelihood of success.

Definitions

- **Cyber Crime** – criminal activities carried out by means of computers or internet

- **Cyber Extorsion** - a nefarious cybercrime where threat actors exploit security vulnerabilities to breach digital security systems and gain unauthorized access to valuable assets. These assets range from confidential data and intellectual property to financial currency and critical infrastructure systems.

Definitions

- **Social Engineering** - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

- **Malware** - Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

- **Ransomware** – Software designed to block access to a computer system until a sum of money is paid.

Don't Be Fooled!

- A common misconception is that nonprofit organizations are not a target for cybercrime. In truth is: nonprofits make a great target for cybercriminals because they offer something of significant value:

  sensitive information on donors, volunteers and support staff

- Many nonprofits think they are not at risk of being a target because they aren't large enough, but their small size is one of the factors that makes them more appealing to cybercriminals.

- Unlike large corporations, nonprofits usually have fewer IT staff and resources, making them particularly vulnerable to cyber-attacks. IT staff at nonprofits frequently juggle several responsibilities, which means they have less time to focus on security.

Why Nonprofits are Targets of Cybercrime

Limited Resources: Many nonprofits operate on tight budgets and may not have the funds to invest in high-end cybersecurity measures. This could leave them more vulnerable to cyberattacks than organizations with more resources to spend on security.

Why Nonprofits are Targets of Cybercrime

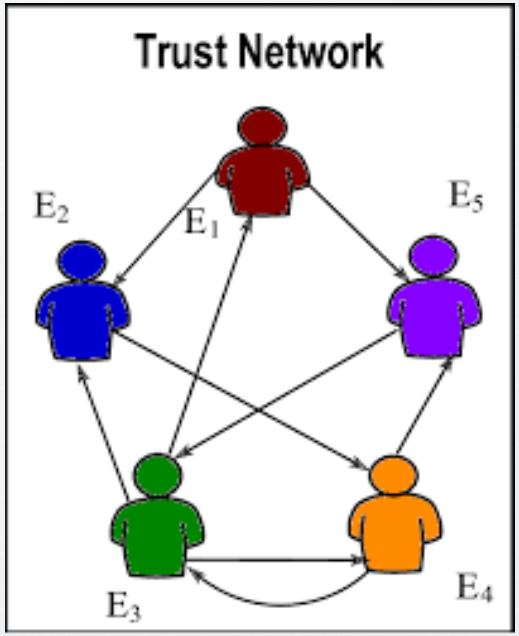
Wealth of Sensitive Information: Nonprofits deal with a lot of sensitive data. This could include contact details, financial information of donors, and personal information about the people they serve. All this data could be a goldmine to cybercriminals who can use it for identity theft or financial fraud.

Why Nonprofits are Targets of Cybercrime

Less Technical Expertise: Nonprofits often focus on their mission rather than tech stuff. This means they might not have staff who are trained to identify and deal with cyber threats. This lack of expertise can leave them exposed to attacks.

Why Nonprofits are Targets of Cybercrime

Trust-Based Networks: Nonprofits work closely with volunteers, donors, and other organizations. Cybercriminals can exploit these relationships, tricking people into revealing sensitive information or clicking on malicious links.



Nonprofits are Unprepared Against Cyberattacks

Nonprofits raise up to $30 billion in funds each year and often don't have the necessary security measures in place, making them attractive to hackers.

9 out of **10** organizations ***DO NOT*** train staff regularly on cybersecurity

3 out of **4** organizations ***DO NOT*** monitor their networks

4 out of **5** organizations ***DO NOT*** have a cybersecurity plan

Nonprofits are Unprepared Against Cyberattacks

The average length of interruption after a ransomware attack is 22 Days...

Consequences are significant and costly, including:

- Identity theft
- Reputation harm/loss
- Precious funds have to be used to recover data
- Holding the organization to scrutiny because of identified vulnerabilities in its cybersecurity
- Disruption in the ability to carry out activities
- Exposing sensitive data on donors and stakeholders

Example #1: International Committee of the Red Cross (ICRC)

In a supply chain attack, cybercriminals used stolen identity data to access the network of a third-party contractor to the ICRC. These hackers were then able to gain access to the networks of more than 60 Red Cross "national societies."

The criminals obtained the sensitive personal information of more than 515,000 individuals including staff, donors, volunteers, first responders, and most insidiously, victims of tragedies from around the world.

One cyber expert stated that this January 2022 attack was the greatest ever security breach of any humanitarian organization.

Example #2: The Philadelphia Food Bank - Philabundance

In a phishing attack, cybercriminals infiltrated the email system of the Philadelphia Food Bank. The scammers used credible information found in the nonprofit's email system to request payment for the construction of a new community kitchen, and Philabundance wired them the funds.

Philabundance was swindled out of approximately 1 million dollars.

PHILABUNDANCE

Driving hunger from our community

Example #3: Blackbaud

Blackbaud is one of the world's largest providers of financial and fundraising technology for nonprofits.

In a supply chain attack, cybercriminals gained unauthorized access to Blackbaud's donor software program for nonprofits called Raiser's Edge. Through sophisticated hacker techniques, these malicious actors were able to avoid detection and were able to access customer data for months.

Blackbaud paid an undisclosed ransomware amount to the cybercriminals to resolve the issue.

Know Your Scams

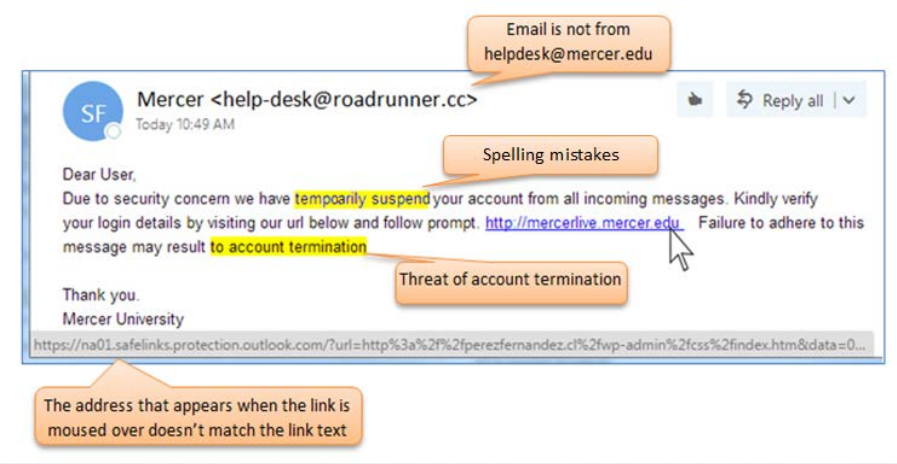
Each of these scams is carried out with the goal of tricking the victim into providing information or clicking on a link, which will install malware onto their device.

- Phishing – carried out via email
- Vishing – carried out via phone
- Smishing – carried out via text or social media
- Spear phishing – targeting phishing in which the fraudster takes time to learn about the victim
- Whaling – targeting executives or presidents with the hope for a bigger return on the phishing investment

Know Your Scams

Phishing - the practice of using deception to get you to reveal personal, sensitive or confidential information

- Spoofed emails and websites



Always:

- Review the greeting
- Look closely at the header
- What is the sender's email address
- Never click on links that are included in email messages

Know Your Scams

Vishing - scam carried out via phone

- spoofing a legitimate phone number
- uses internet phone services (VoIP) to complete the scam
- Combination of 'voice and 'phishing'

Always:

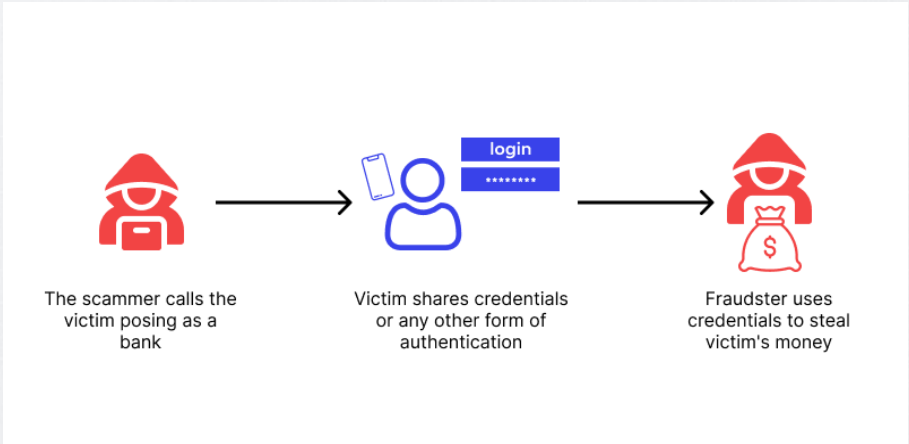
- Be aware
- Don't give into pressure
- Don't answer phone calls from unknown numbers
- Stay calm
- Be skeptical

One form targets your bank account or credit card account:

– *Your account has been compromised. Please call this number to reset your password.*

Other vishing scams include things like:

- Unsolicited offers for credit and loans
- Exaggerated investment opportunities
- Charitable requests for urgent causes
- Extended car warranty scams



Know Your Scams

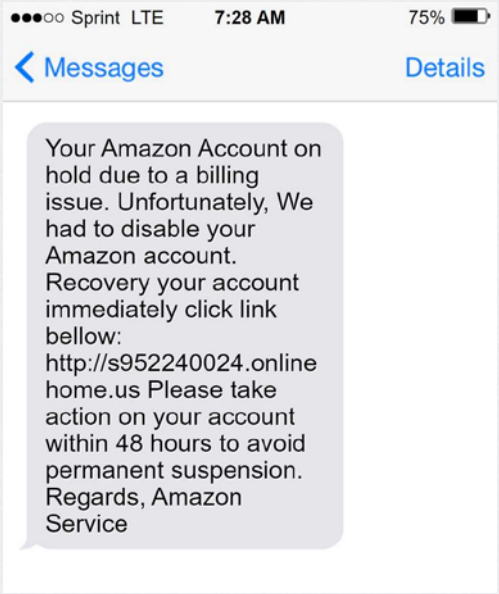
Smishing - scam carried out via text or social media

Combination of 'SMS' (Short Message Services) and 'phishing'

- **Banking Scams:** *"Dear [Bank Name] customer, we've detected unusual activity on your account. Please click the link to verify your transactions: [malicious link]."*
- **Parcel Delivery Scams:** *"Hello, this is [Courier Service]. We've attempted to deliver your package today but failed. Schedule your redelivery here: [malicious link]."*
- **Account Verification Scams:** *"We detected a login attempt from an unfamiliar location. If this wasn't you, please secure your account here: [malicious link]."*
- **Contest Winner Scams:** *"You're the lucky winner of our grand prize! Register here to receive your reward: [malicious link]."*
- **Emergency Scams:** *"A family member of yours has been in an accident. Call this premium rate number for details: [malicious phone number]."*

Best Practices:

- Never click on suspicious links
- Verify independently
- Use phone security features
- Stay updated
- Don't share personal information
- Check for official communications



Know your Scams

Phishing vs. spear phishing vs. whaling

Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing
A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing
A type of phishing that targets individuals.

Whaling
A form of spear phishing that targets high-ranking victims within a company.

Know Your Scams

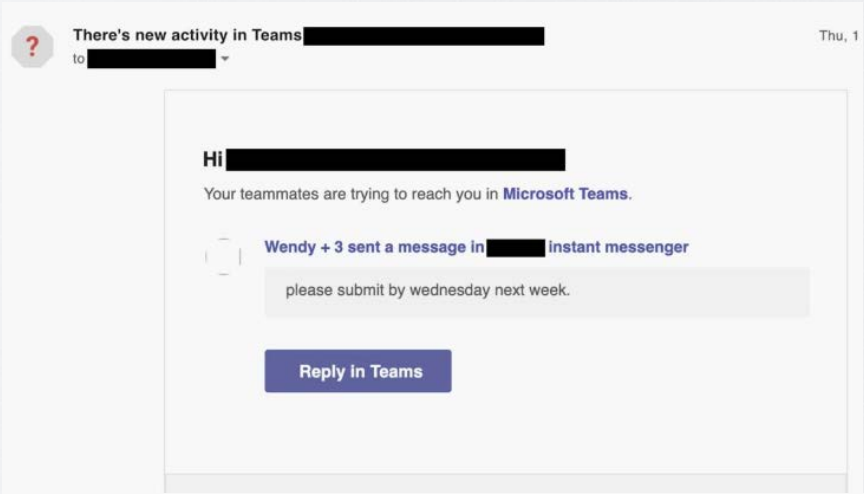
Spear Phishing - targeted phishing, in which the fraudster takes time to learn about the victim.

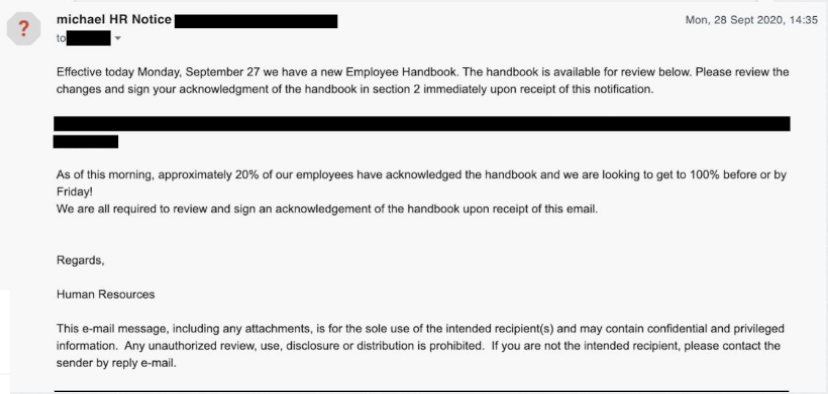
Personalized emails to particular individuals or groups of people with something in common.

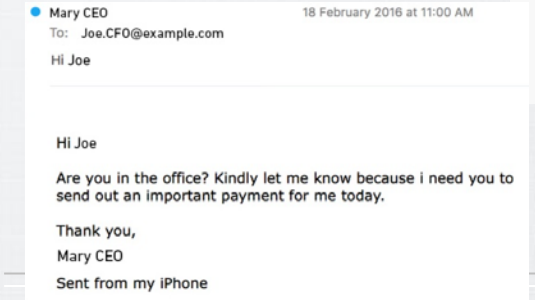
Sole purpose is to get inside the recipient's head and make them think the messages they're responding to are 100 percent legitimate—achieved due to personal touches designed to make them think what they're dealing with is the real deal.

Prevention:

- Two-Factor Authentication
- Password management policies
- Educational Campaigns







Know Your Scams

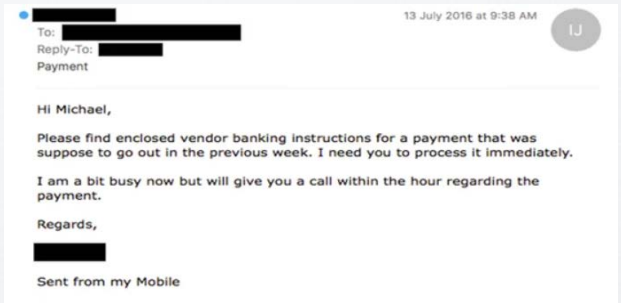
Whaling - targeting executives or presidents with the hope for a bigger return on the phishing investment.

Whaling phishing emails often consist of:

- A sense of urgency
- Personalized information about the target and/or organization
- Corporate/business tone of voice and jargon

Best Practices:

- Educate employees
- Flag emails from outside the organization
- Discuss social media use with team
- Establish multi-step verification for all requests for sensitive date or wire transfers
- Exercise data protection and data security policies
- Follow up phone call


[redacted]
13 July 2016 at 9:38 AM
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

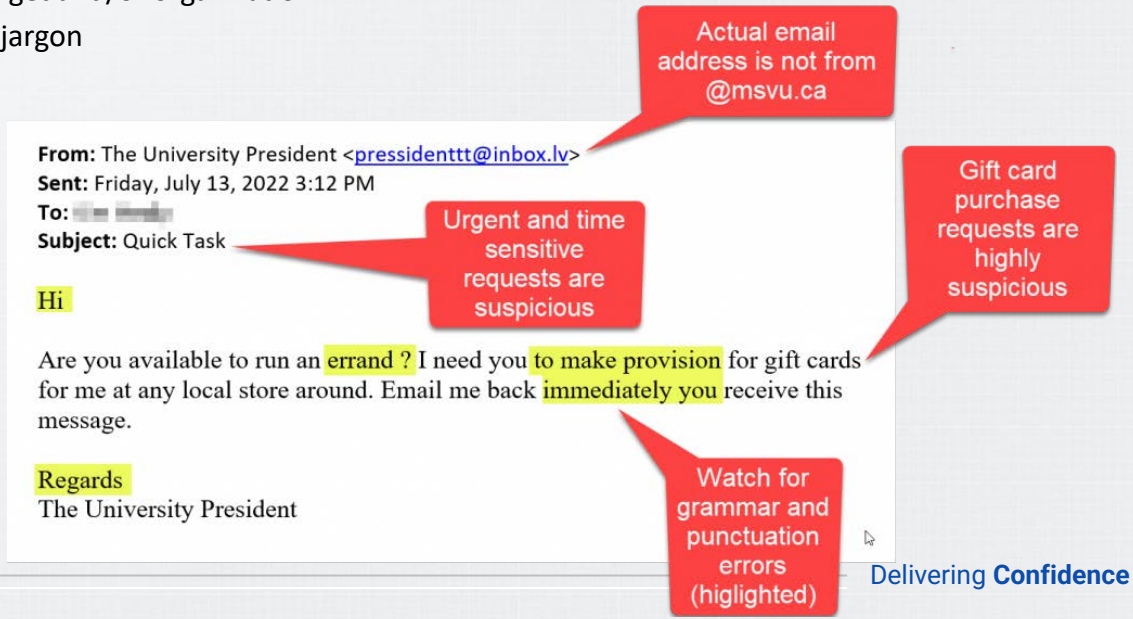
Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile



Social Media

Failing to prioritize the security and privacy of a social media account can result in negative consequences spanning both the personal and professional worlds.

By asking seemingly random questions, malicious actors can use social engineering to obtain the information necessary to answer security questions required to reset a password (e.g., the name of a first pet, mother's maiden name).

For example, a malicious actor could leverage information gleaned from social media accounts about an upcoming class reunion. Posing as a classmate, the malicious actor could increase the likelihood of success in an email compromise through the use of a tailored phishing email campaign. This believable impersonation effort would allow the threat actor to gain the trust of the target account holder and leverage it for malicious purposes.

Know Your Scams

- Safeguarding user IDs and passwords
- Enabling two or multifactor authentication when possible
- Never clicking on communications from unknown sources
- Running training simulations for phishing, vishing, smishing, spear fishing, whaling and business email compromise
- Keeping current with hardware and software updates
- Be mindful of what you store on your devices and how you do it

BE SKEPTICAL!!

Establish Anti-Fraud Culture – Fraud Policy

The tone from the top is a key part of any fraud prevention and detection strategy.

A fraud policy should include these key elements:

- An explicit definition of actions that are deemed to be fraudulent
- Allocation of responsibilities for the overall management of fraud
- A statement that all appropriate measures to deter fraud will be taken
- The formal procedures which employees should follow if a fraud is suspected
- Notification that all instances of suspected fraud will be investigated and reported to the appropriate authorities
- An unequivocal statement that all fraud offenders will be prosecuted and that the police will be assisted in any investigation that is required
- A statement that all efforts will be made to recover wrongfully obtained assets from fraudsters
- Encouragement to employees to report any suspicion of fraud
- The steps to be taken in the event a fraud is discovered and who is responsible for taking action including:
  - procedures staff should follow
  - assigning responsibility for an instant response to the occurrence recovering funds
  - dealing with the media
  - preserving evidence and reporting to the police

A fraud policy raises awareness amongst staff that response plans have been devised, to deal with and minimize the damage caused by any fraudulent attack. By explicitly defining actions that constitute fraud you ensure that all employees and third parties are aware of what is and is not acceptable.

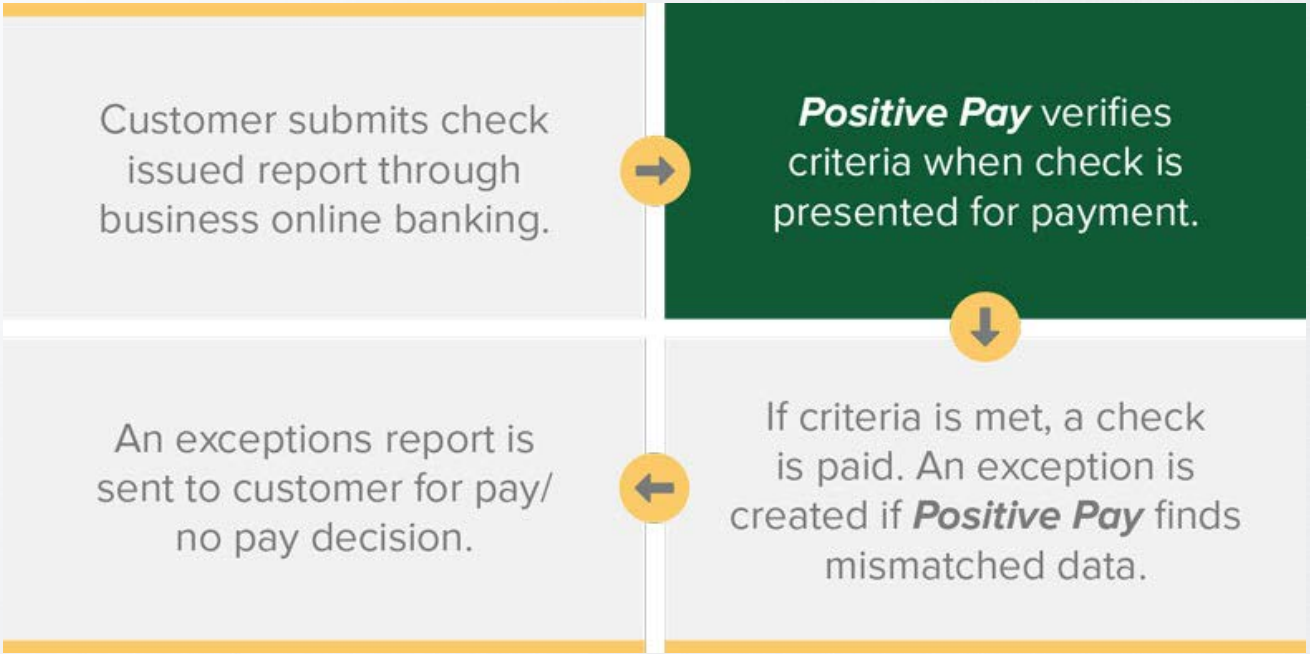
Practice Good Cyber Hygiene

Cyber hygiene is a set of best practices organizations perform regularly to maintain health and security of users, devices, networks and data.

- **Passwords**
- **Multifactor authentication**
- **Secure your network firewall**
- **Anti-malware and antivirus programs**
- **Update operating systems and apps**
- **Get a reliable VPN**
- **Backup your files**
- **Delete suspicious emails or messages**
- **Completely remove all data from old devices**
- **Stay on top of your cyber security**

Best Practices to Implement

Consider Implementing Positive Pay - Positive Pay is an automated Cash-management service used by financial institutions to deter check fraud.



Best Practices to Implement

RISK TERMINOLOGY

THREAT: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, assets, individuals, other organizations, or society

VULNERABILITIES: A characteristic or specific weakness that renders an organization or asset open to exploitation by a given threat

LIKELIHOOD: Refers to the probability that a risk scenario could occur

RISK: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences

- **Train staff regularly:** Online security training should be a regular occurrence that includes all staff across the organization, including volunteers with online access.
- **Protect passwords:** Instruct staff to change passwords often or put software in place that requires passwords to be changed and stress the importance of not recycling passwords across multiple websites and social media platforms.
- **Update software regularly:** At a minimum, systems should have strong spam email filtering, antivirus software and financial malware detection software. This software should be updated and patched regularly for the best defense

Best Practices to Implement

- **Regularly backup systems:** Maintain regular backups of critical data to protect against system failure and ransomware attacks. Disconnect external backup drives from your machine when not in use.
- **Restrict privileges:** Limit the number of people who have administrative privileges that allow them to make changes to systems. The more people who have access to this ability, the greater chance of a cybercriminal obtaining these sensitive credentials.
- **Use multi-factor authentication:** Require that users enable multifactor authentication when signing into their online accounts.

Best Practices to Implement

- **Verbally validate payment instructions:** It's always best to pick up the phone and communicate with the relevant parties to confirm requests.
- **Create a disaster recovery plan:** The actions and corresponding roles to take if systems are compromised should be clearly documented and understood.
- **Consider an insurance policy:** Insurance for cybersecurity typically includes first-party coverage of losses incurred through data destruction, hacking, data extortion, and data theft. Policies may also provide coverage for legal expenses and related costs.

Best Practices to Implement

Consider Outsourcing IT Services - Nonprofits don't always have a dedicated IT employee – by outsourcing IT functions, key personnel can focus on the mission and leave the cyber security and other imperative IT functions to the experts.

Free Resources

- FBI
- Cybersecurity and Infrastructure Security Agency (CISA)
- ACFE
- AICPA

ACFE®
Association of Certified Fraud Examiners

CISA
CYBER+INFRASTRUCTURE

AICPA®

Kaitlyn H. Axenfeld, CPA/CFF, CFE
Audit Partner

Email: kaxenfeld@dmcpas.com

Web: www.dmcpas.com

Address:

DM Financial Plaza
221 S. Warren St.
Syracuse, New York 13202-1628

Phone: (315) 472-9127, ext. 207

Christine N. Petrone, CPB
Accounting & Advisory Services Department Supervisor

Email: cpetrone@dmcpas.com

Web: www.dmcpas.com

Address:

DM Financial Plaza
221 S. Warren St.
Syracuse, New York 13202-1628

Phone: (315) 472-9127, ext. 246

Copyright / Disclaimer

This presentation and any related materials are designed to provide accurate information in regard to the subject matter covered, and are provided solely as a teaching tool, with the understanding that neither the instructor, author, publisher, nor any other individual involved in its distribution is engaged in rendering legal, accounting, or other professional advice and assumes no liability in connection with its use. Because regulations, laws, and other professional guidance are constantly changing, a professional should be consulted if you require legal or other expert advice.

Circular 230

Any tax advice contained herein was not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code or applicable state or local tax law provisions.