CERINI & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS

2020 Nonprofit Update

IT Concerns of Going Virtual

SHARI DIAMOND
PARTNER, CERINI & ASSOCIATES, LLP

CERINI & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS

CONNECTED TECHNOLOGY

KEVIN URSO
PRESIDENT, CONNECTED TECHNOLOGY, LLC

Introduction and Objectives

- Information flow and internal control considerations
- Policies and procedures
- Assessing hidden dangers with email, social media
- Securing your workspace
- Top 10 things to do when working remotely
- Microsoft 365 for non-profits

Objectives of Internal Controls

- Accurate Financial Information
- Compliance with Policies and Procedures
- Safeguarding Assets
- Efficient Use of Resources
- Accomplishment of Company Objectives and Goals

- Institute of Internal Auditors (IIA)

What Internal Controls Do

Effectiveness and Efficiency of Operations

- addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources.

Reliability of Financial Reporting

- preparation of reliable financial statements and publicly reported financial data.

Compliance with Laws and Regulations

- compliance with those laws and regulations to which the entity is subject.

-COSO Integrated Framework Executive Summary

Why Internal Controls Are Important

- Provides management with confidence that the entity is operating according to standards which are monitored-someone is watching.
- Indicates to staff that what they are doing is important and that QUALITY is important.
- Sends a signal that certain behaviors will not be tolerated.

Information and Communication

- Information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.
- Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business.
- To achieve effective communication, information must flow down, across, and up the organization.
- There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders (don't forget training).

-COSO Integrated Framework Executive Summary

Information Flow and Internal Controls

- Understanding your data and what information is critical to your organization's success
  - Where does this data live?
  - Where does this data travel to?
  - Who is responsible for ensuring the data remains intact (completeness & accuracy)
  - How did this change as a result of working virtually
- Key business control processes
  - Approval for key business transactions (e.g., payroll, purchasing, accounts payable)
  - How are managers able to properly assess and approve documents
  - How are your users working
    - Same for your vendors and your clients
  - Did you have to revise any internal operations

Policies and Procedures

- What policies are in place for your users when accessing your data
  - Acceptable use (should include working remotely)
  - Data confidentiality
  - Remote access (vendors and clients)
  - Backup and Recovery
  - Security Breach and Notification
  - Social media
- Documented procedures for working remotely AND key business processes
  - What if certain key staff are not able to work
    - Cross-training
    - Re-assigning authority (access permissions)
  - How are employees accessing your data
  - **TRAINING!**

Cybersecurity Threats

- Checkpoint: 200,000 Coronavirus-related cyber attacks - a 30% increase from the weeks before
- Steven Inch, a global security manager with HP said since the COVID-19 pandemic hit, the number of cyber and hacking attempts have skyrocketed across the globe at “about a 600% increase”
- In April 2020, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to other working on the novel coronavirus response
  - The number of cyber attacks is now more than 5 times the number directed at the WHO in the same period last year
- Google reports 18 million daily phishing attempts

Cybersecurity Challenges

- One of the primary ways computers and systems are being hacked is via fake emails that entice you take some action (phishing)
  - Clicking on a link
  - Downloading or opening an attachment
- Other methods include fake online ads on social media, websites, or browser pop-ups
  - Once clicked, they can install malware (malware clickbait)
- Small to medium size businesses don't have the sophisticated security systems in place to defend against cyber attacks
- With rapid movement to working at home, many of the security layers were removed overnight.
- This pandemic is also putting a spotlight on the fact that most companies don't do a good job of just basic security hygiene.

Phishing Emails

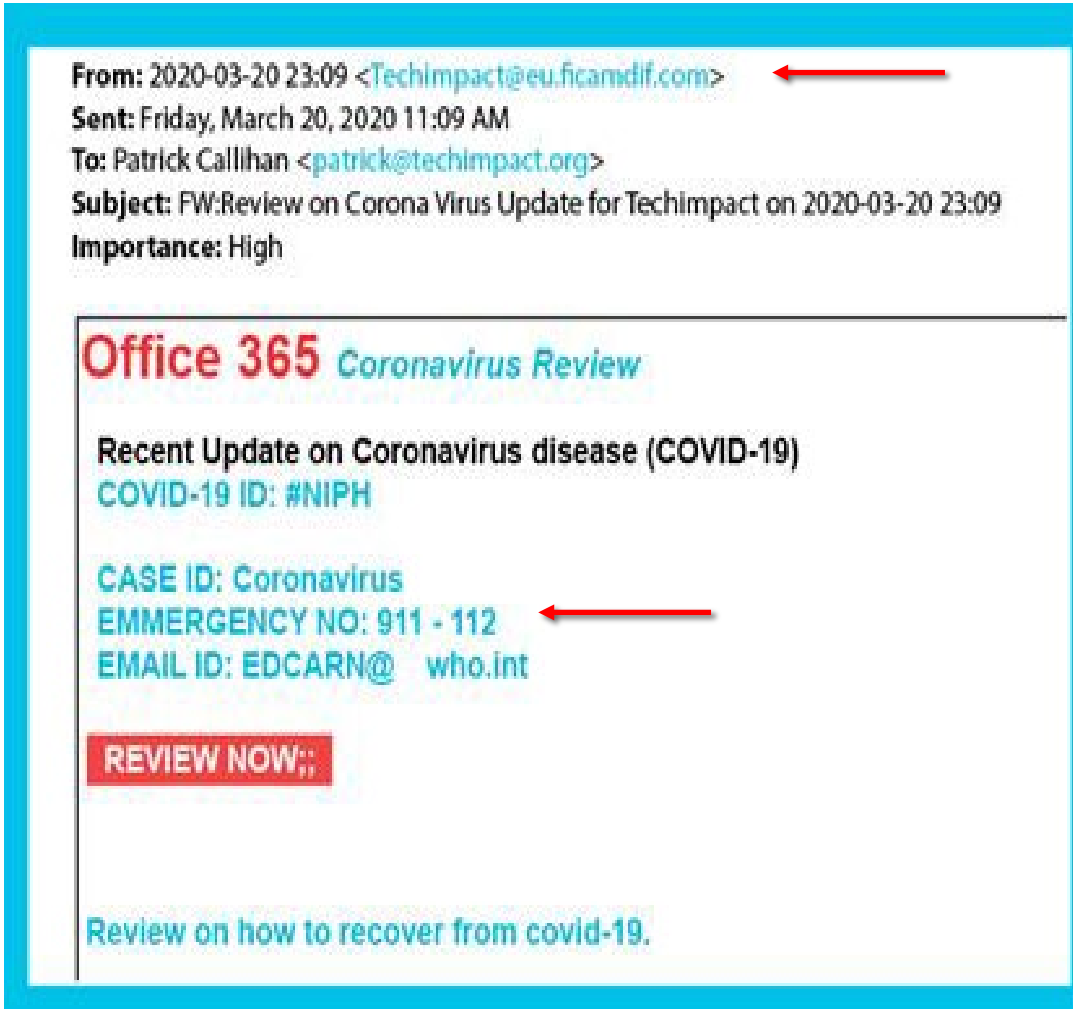
Phishing emails are designed to trick an unsuspecting person into providing sensitive information that can give them access to both organizational and personal data — TechSoup and Tech Impact staff have been receiving phishing emails daily over the last several weeks.

Some are fairly obvious→

Phishing Emails

If you look closely at the email, there are a few things that suggest it is a phishing attempt.

- The first sign is that the email references Office 365 but does not come from either Microsoft or a legitimate company that offers Microsoft services.
- The content itself is also suspicious because there are typos and it uses an unknown email ID.



Malicious Emails

Others are a bit sneakier, in which hackers try to pose as someone within your organization. In this case, the hacker used a custom field to pose as an HR staff member asking the recipient to click through to a required training.

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require al employees to read and acknowledge the policy before [[current_date_1]].

If you have any questions or concerns ragarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

Malicious Emails

- Hackers use publicly available information on websites, including your own nonprofit website, to identify key information that can be used to trick you, such as your email domain and senior staff names.
- The email actually looks like it is coming from your HR manager, and the individual's name may even be spoofed in the “From” field of the email and the content of the email.
- However, if you look at the actual From email address, you will notice that it does not actually come from that individual.
- Always be suspicious of an email coming from your CEO, HR, or others if there is a request for action of any kind. It can be a phishing attempt.

Other Types of Scams

App scams: Scammers are creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.

Charity scams: Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.

Treatment scams: Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19. Scammers are also posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), tricking recipients into downloading malware or providing personal identifying and financial information.

Supply scams: Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.

Provider scams: Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19 and demanding payment for that treatment.

Other Types of Scams

Investment scams: Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result.

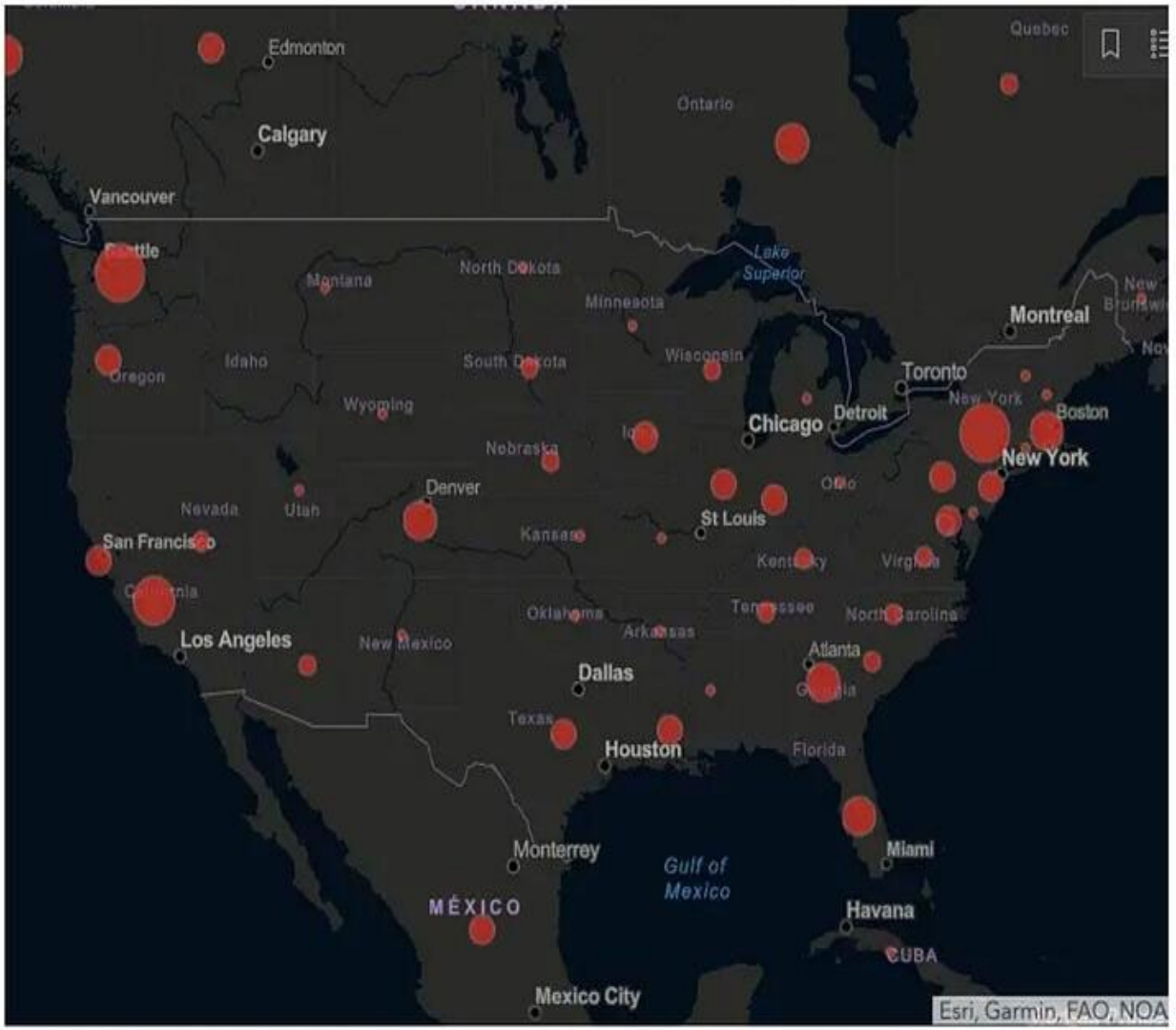
COVID-19-specific scams: There is a lot of phishing activity related to COVID-19 that asks people to provide information in order to access benefits or information. These are examples highlighted by KnowBe4:

- Coronavirus Stimulus Package (SSN): Claims that the person is eligible for a $1,200 stimulus check, and they just need to enter their Social Security number to confirm.
- Coronavirus Testing Kit (SSN): Claims that due to new government regulation, the person can receive a free coronavirus testing kit sent to their home.
- Coronavirus School Schedule (SSN): Targets parents by referencing a change in their child's school schedule due to the coronavirus, then asks for the Social Security number to confirm identity.
- Increased Coronavirus Cases in Your Area (zip code): A call from the local "county commissioner" claims that there has been an increase in coronavirus cases in their area and requests their zip code to confirm their location.

Malware Clickbait

Cybersecurity researchers have identified several fake COVID-19 tracker maps like this one that infect people's computers with embedded malicious code when you click on the image to open it.

The tactic is one of many ways hackers and scammers are capitalizing on people's fears about COVID-19 to spread malware.



Johns Hopkins University maintains a coronavirus dashboard that's one of several safe options for keeping up with the spread of the virus. Johns Hopkins

Strategies for Strong Remote Operations

- ☑ Change default WiFi passwords
- ☑ Change default router passwords
- ☑ Update software regularly
- ☑ Ensure a Virtual Private Network (VPN) is used
- ☑ Separation of private and personal technology
  - this is often the biggest hurdle and may come with some costs
- ☑ Use Multi Factor Authentication
- ☑ Have a corporate policy for cloud-based file sharing systems and know where corporate data is being stored
- ☑ Monitor how data leaves your organization
- ☑ Have internal monitors and alerts in place to warn of potential problems
- ☑ Don’t allow the use of administrator privileges on a regular basis

Top 10 Things to Do to Stay Secure

1) Implement a Backup up and business continuity system
2) Conduct continual employee training on current cyber threats.
3) Implement very good firewall with next generation features.
4) Require a strict password policy.
5) Regularly monitor network and security logs.
6) Have had a third party conduct annual threat audits.
7) Perform O/S, software and plug-ins updates and patches regularly.
8) Implement malware and anti-virus software that is monitored.
9) Don't allow Personal devices that are not vetted.
10) Do not allow Admin credentials in daily use.

Don’t forget: Cybersecurity training for all users!

Microsoft 365 for Non-Profits

M365 Business

- Microsoft 365 Business offers a single, integrated solution that combines the productivity apps users know and love with device management, advanced security features, and an always up-to-date Windows OS
- Microsoft has a special offer that provides nonprofits with free M365 Business for up to 10 users, and discounted pricing of $5 per additional user per month (M365 Business is typically $20 MSRP)
- Send Kevin an email and he will send you an M365 for nonprofits ebook

CONTACT INFO

Kevin Urso
President
Connected Technology, LLC
7 Flowerfield Suite 30
Saint James, NY 11780
Phone: 631-724-6504
kurso@connectedtechnology.com

Shari Diamond, CIA
Partner, Internal Audit
Cerini & Associates, LLP
3340 Veterans Memorial Hwy
Bohemia, NY 11716
(631) 582-1600 x243
sdiamond@cerinicpa.com