

September 2020

---

# Rogers-Lowell Chamber of Commerce

"Quick Wins on Securing Your Remote Workforce"

## **The Edafio Difference**

The Edafio Difference goes beyond words. It is a culture embraced by all of our associates. It is our drive to enable our client's success. It is our focus to treat each other, and especially our clients, with humility and respect and it is a relentless focus on integrity in all that we do.

## **Leading IT provider & Consulting Firm**

Arkansas-based full-service technology, cybersecurity, cloud-computing and healthcare consulting company since 1999

## **Arkansas Presence**

Offices located in North Little Rock, Conway, and Rogers

## **Long-term partnerships**

Supporting 200+ mid to enterprise-level clients across healthcare, financial services, retail, and transportation in Arkansas and the surrounding states.

## **Recognition**

Recognized as a top Managed Service Providers and Consultants in North America

# Cheryl Hearne

## Senior Cybersecurity Consultant

Cheryl collaborates with clients to proactively move the needle on their information security posture and responds to incidences that could impact the objectives of the organizations she is committed to protecting.

Cheryl believes that her diverse background across multiple industries has provided her with the ability to succinctly evaluate and prioritize cybersecurity strategies. She has earned multiple certifications to include a CISSP, GPEN, Sec+, Net+, and PCI ISA.

Cheryl shares her passions around data privacy with any family member or friend who can listen without their eyes glazing over. She indulges the creative side of her brain through photography, playing the guitar, and travelling as much as possible.



# Angeline Button

## Senior Cybersecurity Consultant



Whether it's phishing, malware, ransomware, or user error, the potential for serious breaches in the security continues to grow and Angeline is passionate about collaboration with a one-team approach whether it is through teaching, investigating or implementing security solutions to protect businesses and people.

Angeline received the 2018 RH-ISAC Breakthrough Female in Cybersecurity Peer Choice Award and has held positions such as a Web Administrator and Practice Lead of Threat Intelligence & Hunting.

Angeline enjoys hiking with the family throughout Arkansas with her two children, the oldest an attorney and the youngest (at 13) an avid fencer and her miniature schnauzer, Professor Snape.



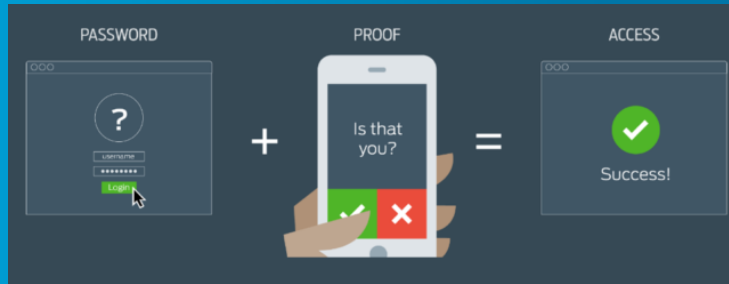
# Tips for Cybersecurity At Home

- 07** MFA or 2FA
- 09** Software Updates
- 10** Passwords & Default Accounts
- 12** Anti-Virus
- 13** VPN & Guest Networks
- 17** Phishing & Email Hygiene
- 23** Disable Microsoft Macros
- 26** Cyber Insurance

**How can we improve our  
employee's cyber risk while  
working remotely?**

**Enabling MFA (or 2FA) can  
ensure your accounts are up  
to 99.9% less likely to be  
compromised.**

---



## Enable Multi-Factor or Two Factor Authentication

# MFA

- 
- ✓ Codes sent to an email address
  - ✓ Codes sent via SMS to your phone
  - ✓ Codes generated by smartphone app
  - ✓ Fingerprints
  - ✓ Facial Recognition
  - ✓ Behavior Analysis



# Software Updates

---

## Personal

- ✓ Keep up with patches and updates for work and personal devices (Windows 10, MAC, Applications, Browser Addons)
- ✓ Remove unnecessary software (i.e., Xbox Live on Windows)

## Work

- ✓ Create secure checklists or standard images for new devices
- ✓ Automate patch management where possible



# Passwords

- ✓ Passphrases:  
"G!ueC@rM0dleH0bb1e" or  
"I love NFL football!"
- ✓ Passwords: At least 12  
characters with capital and  
lowercase letters, symbols, and  
numbers
- ✓ Never use the same password  
twice
- ✓ Create and store unique  
passwords using a password  
manager



# Default Accounts

## Network Accounts

- ✓ Router Account – Find the default on the manufacturer's web site
  - ✓ Modem Account – Find the default on the underside of the device or contact your ISP
  - ✓ Review steps from ISP on how to change
- 

## System Accounts

- ✓ Disable default admin and guest accounts.
- ✓ Create separate administrator accounts and never use them to surf the internet

# Anti-Virus

Secure your devices with anti-virus software & keep it updated.

Name	Free Version	Paid Version	Details
BitDefender	Yes	Yes	Free & paid version has the same core Anti-Virus protection. Free Version offers Web Protection. MANY Additional/Enhanced features in Paid Version. <b>Free version does NOT support MAC devices.</b> <b>Free Version does not include Parental Controls.</b>
Sophos Home	Yes	Yes	Free version has excellent scores in independent testing. Free version has web filtering and browser features. Free Version includes Parental Controls. <b>Free version limited to 3 devices.</b>
Microsoft Windows Defender	Yes	No	Built into Windows 10. Good lab scores. <b>Limited to Windows.</b> <b>Web protection only works on Microsoft Browsers.</b> <b>Awkward Scan Scheduling</b>

- # VPN



# Guest Networks

---

Writing down a wireless network password is risky. Sharing it with family or friends who may inadvertently download malicious software into your network creates even more risk.

Enable a guest wireless network to protect your home network.

Contact your Internet Service Provider (ISP) for more information on how to get one set up at home.





---

# Confidentiality

Protect confidential or sensitive information while you're working from home.

Consider turning off digital personal assistants such as Alexa and Siri.

Be aware of family or friend's exposure to work calls and video conferences.

# What are the most common email vulnerabilities for my organization?



Over **90%** of data breaches  
started with **Phishing emails.**

---

# Security Awareness

---

Your employees are your organization's last line of defense against the bad guys. Use a Security Awareness Program to safely phishing and train your users to strengthen your **human firewall**.

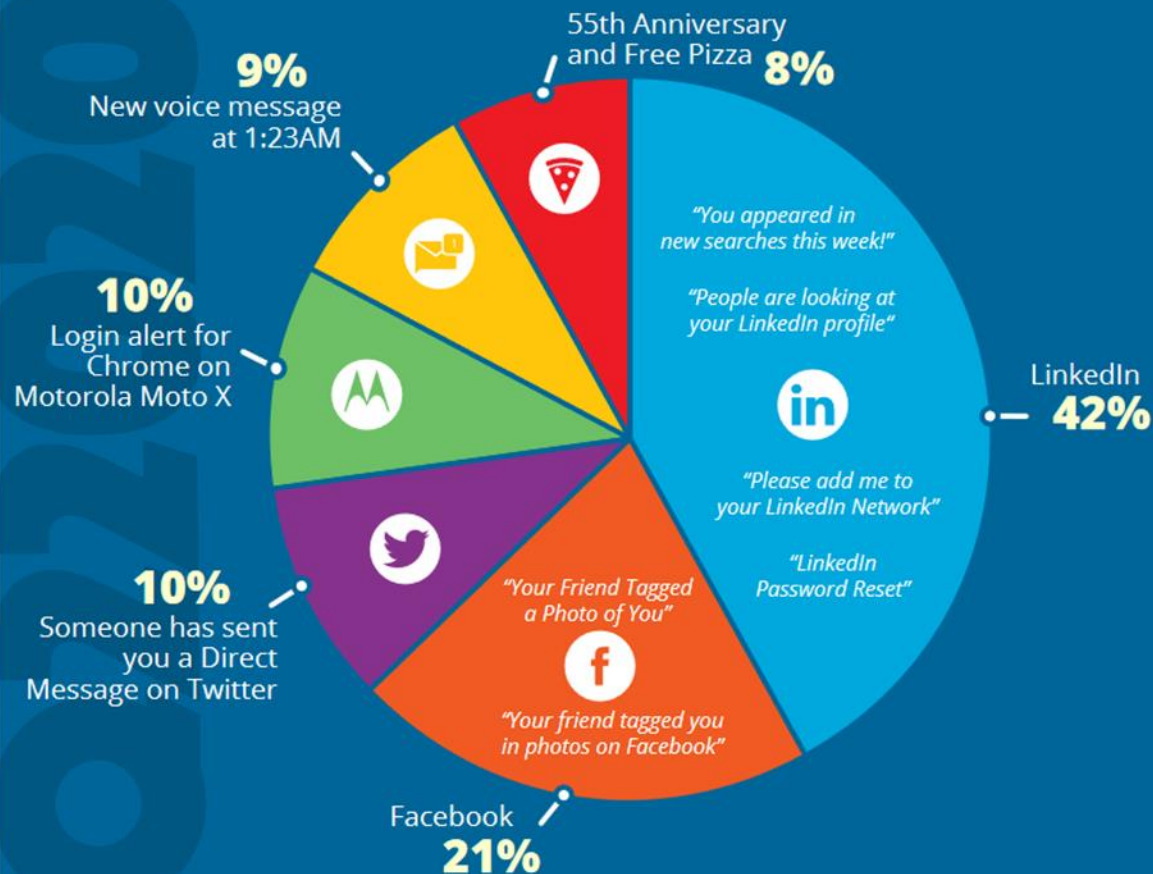
Organizations that must comply with regulatory frameworks such as:

- PCI (Payment Card Initiative)
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- Sarbanes-Oxley reporting requirements
- NIST or ISO

Even though it may not be a requirement for your business, remember that **94%** of SMBs detected malware was received by email. This includes Ransomware.



# TOP SOCIAL MEDIA EMAIL SUBJECTS













## KEY TAKEAWAY



LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or mentioned you can make someone feel special and entice them to click. And everyone loves free pizza!

# TOP 10 GENERAL EMAIL SUBJECTS

	Password Check Required Immediately	20%
	Vacation Policy Update	12%
	Branch/Corporate Reopening Schedule	11%
	COVID-19 Awareness	10%
	Coronavirus Stimulus Checks	10%
	List of Rescheduled Meetings Due to COVID-19	10%
	Confidential Information on COVID-19	8%
	COVID-19 - Now airborne, Increased community transmission	7%
	Fedex Tracking	6%
	Your meeting attendees are waiting!	6%

## KEY TAKEAWAY



Hackers are playing into employees' desires to remain security minded. Unsurprisingly, half of the top subjects for this quarter were around the Coronavirus pandemic. Curiosity is also piqued with security-related notifications and HR-related messages that could potentially affect their daily work.

# Social Engineering Red Flags



## FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



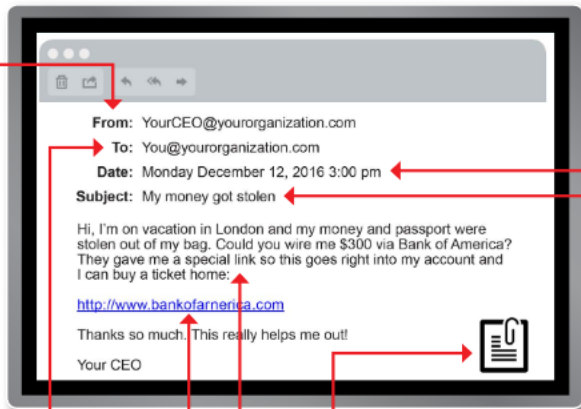
## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofarnerica.com](http://www.bankofarnerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



## SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



## ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.



## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

---

# Email Hygiene



“What data would be available if one of my organization's employee's email accounts were compromised?”

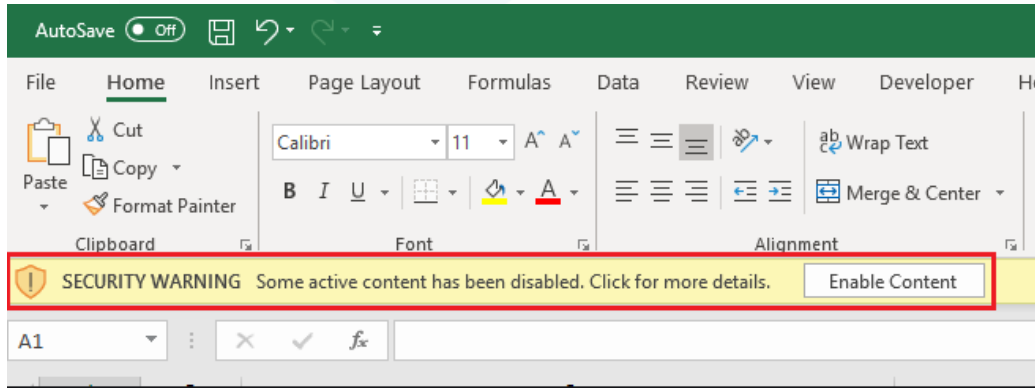
- Data Retention Policy
- Allow external forwarding of work emails?
- Allow employees to install Apps or Extensions for their email account?
- Email banner notifying employees an incoming email is outside the organization

The 2019 Verizon Data Breach Investigations Report found that **90%** of emailed malware is distributed via macros.

---

# Microsoft Office Macros

- ✓ Don't enable macros on documents received from untrusted senders.
- ✓ Be Careful with documents from people you trust – in case they've been hacked!
- ✓ Disable all macros in Microsoft Office programs as a default, if possible.

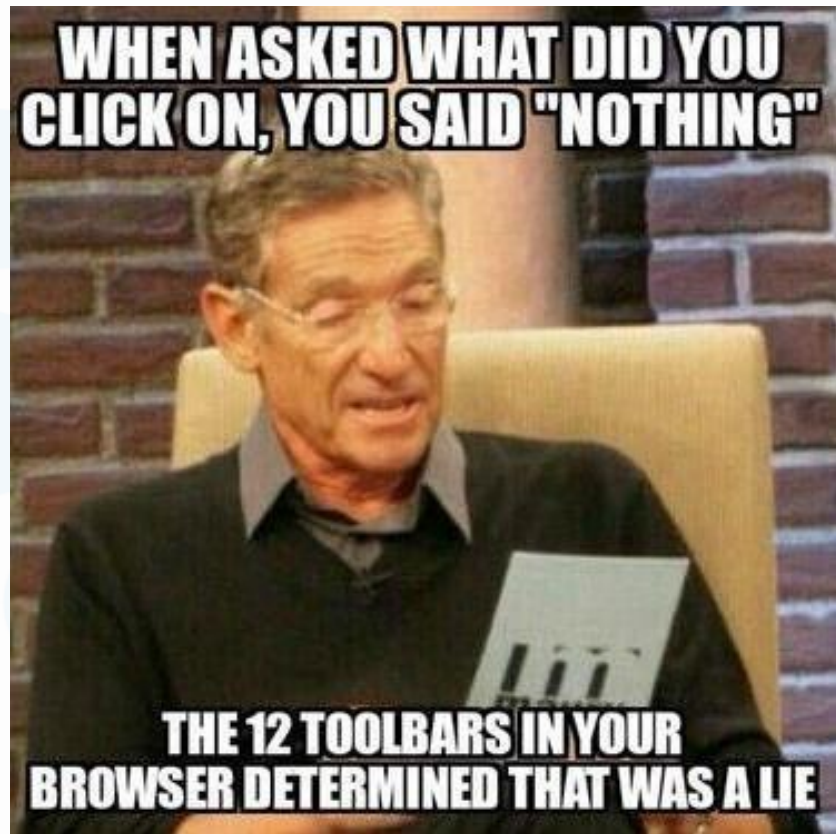


## IMPORTANT

WHEN YOU CHANGE YOUR MACRO SETTINGS IN THE TRUST CENTER, THE MACRO SETTINGS ARE NOT CHANGED FOR ALL YOUR OFFICE PROGRAMS.

ENTERPRISE POLICIES CAN ALSO BE SET TO DISABLE MACROS.





# Why your organization needs to think about Cybersecurity Insurance.

There was a **424%** increase in  
new *SMALL* business cyber  
breaches last year.

---

# HAS YOUR ORGANIZATION CONSIDERED THE BENEFITS OF CYBERSECURITY INSURANCE?

Conventional business insurance policies, like general liability, crime, and professional liability may only afford **SOME** degree of protection.



**60%** of small businesses that  
are victims of a cyber attack  
go out of business within six  
months.

---

# Cybersecurity Insurance

## REMEMBER YOUR DIGITAL ASSETS ARE IMPORTANT TOO

Only a cyber policy is designed to respond to cyber attacks

### CYBER POLICY SHOULD COVER:

- Forensic costs
- Call centers
- Crisis management costs
- Theft of private information
- Notification expenses
- Credit and ID Monitoring
- Data Breach Coach
- Extortion costs

## DATA BREACH COST ESTIMATE

### HOW MUCH WOULD A DATA BREACH OF 6,000 RECORDS COST? \$700,100\*

This is based on a breach of 6000 records containing PII and PHI of both employees and patients:

• Data Breach Coach	<b>\$50,000</b>	• Forensics	<b>\$60,000</b>
• Crisis Mgmt. & PR	<b>\$40,000</b>	• Call Center	<b>\$4,200</b>
• Notification	<b>\$10,000</b>	• Credit Monitoring	<b>\$6,700</b>
• Regulatory Fines & Defense	<b>\$530,000</b>		

\*Note the \$700k does **NOT** include costs associated with loss of productivity, reputational damage, or litigation. You don't have to take our word for it, [run the numbers yourself](#).

# Cybersecurity Insurance

---

Cyber policies are non-standard, vary widely by carrier, and evolve rapidly. Therefore, they should be *re-shopped annually*.

Insurance applications should have all answers documented **OUTSIDE** of the application itself.

This is your proof of attestation.

If there is a concern with the answer being appropriate that item should be discussed in detail with the broker.

These items are crucial to prevent a failure in coverage due to an inaccurate attestation.



# Thank You

---

Visit **edafio.com/blog** for more information

chearne@edafio.com

abutton@edafio.com