THE FULCRUM GROUP
One Technology Solution: Yours

End User Cybersecurity Best Practices

TAWWA Customer Service Workshop

Presented by David Johnson
October 20th, 2022

Texas AWWA
American Water Works Association

Agenda

- Who is Fulcrum Group?
- What's at Risk?
- What to Expect
- Some Best Practices
- Q&A

THE FULCRUM GROUP
One Technology Solution: Yours

Who is Fulcrum Group?

- Started in 2002, Steve Meek & David Johnson - owners
- SPOT Managed IT Services – started in 2008

SPOT Managed IT Services

Primary Offerings

- IT Outsourcing Managed Services
- Cloud Solutions
- VOIP Communications
- IT Infrastructure Projects
- Managed Cybersecurity Services

DIR Texas Department of Information Resources

Channel Futures SMB HOT 101 AN MSP 501 LIST

Small Business of the Year 2017

SANGOMA

CRN MSP 500 2021

THE FULCRUM GROUP

Cybercriminals take advantage of your trust, fear, greed, and plain old human error.

Security awareness training teaches you to spot fakes, avoid risks online, and use good cyber-hygiene practices at work and at home.

WHY DOES IT MATTER?

- The world is getting more digital
  - *Business, banking, healthcare, etc. is all online*

- Crime is following the same trend
  - *Worldwide ransomware attacks*
  - *High-profile hacks in the news*
  - *Phishing emails are more sophisticated each day*

- New privacy laws and regulations are being enacted
  - *Many industries require training for compliance*

WHY SHOULD YOU CARE?

- Because the online world is so interconnected, everyone is a target
- If just one of your accounts gets breached, criminals can use it to breach others
- Criminals may target personal accounts and data to breach corporate ones, and vice versa
- Fraud and identity theft doesn't just affect an individual; it can affect your family, friends, coworkers, and business

WHAT KINDS OF THREATS ARE THERE?

- Phishing and spear-phishing attacks
- Business email compromise
- Social engineering scams
- Common malware and ransomware
- Fake websites that steal data or infect devices
- And much more

It’s not that dangerous online, though, right?

1 in 50 URLs is malicious[1]

Nearly 1 in 3 phishing sites uses HTTPS to appear legitimate[1]

90% of the malware businesses encounter is delivered via email[2]

Most breaches involve phishing and using stolen credentials[2]

[1] Webroot Inc. “2019 Webroot Threat Report: Mid-Year Update.” (September 2019). [2] Verizon. “2019 Data Breach Investigations Report.” (May 2019)

How bad is the risk?

01 Local government faces nearly the same or higher level of risk as enterprise organizations[1]

02 The average total cost of a data breach is now up to $3.92 **million**[2]

[1] 2019 Hiscox Cyber Readiness Report
[2] IBM. "2019 Cost of a Data Breach Report." (July 2019)

What's at Risk?

- Data & Applications
  - Public Safety, Courts, Utilities
- Reputation & Public Confidence
- Critical Infrastructure - Utilities
- Downtime
- Loss of Revenue
- Cost of Recovery

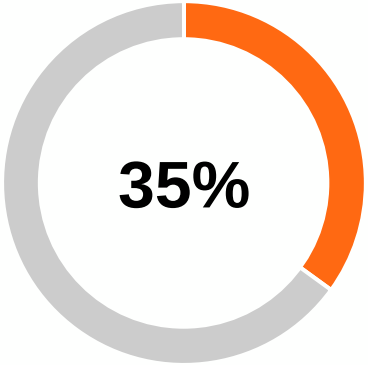
NATIONAL SECURITY

What We Know About The Ransomware Attack On A Critical U.S. Pipeline

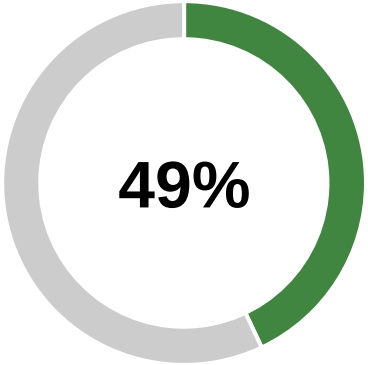
May 10, 2021 · 9:30 AM ET

SCOTT NEUMAN

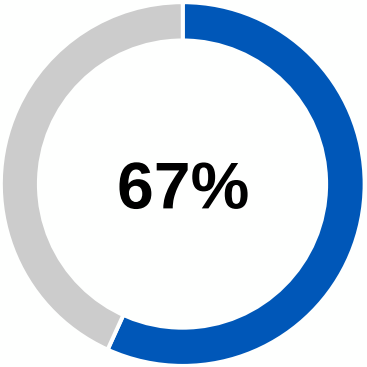
But people know better, right?



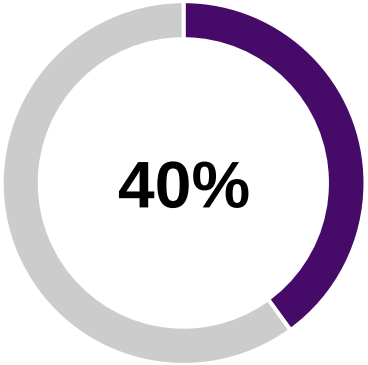
of workers who know they've been hacked don't bother to change their passwords afterward[1]



of employees admit they click links in messages from unknown senders during work[1]



of workers are sure they've received at least one phishing email at work[1]



Of those who received a phishing email, ~40% didn't report it

[1] Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (September 2019)

How does Security Awareness Training help individuals?

It gives you the know-how to stay safe from cybercrime…

AT HOME

- Protect your identity and personal data from theft and fraud
- Secure your devices against viruses and malware
- Keep yourself and your family safe from hackers and spies

AT WORK

- Prevent corporate network infections
- Stop business email compromise
- Keep critical business data safe

How does Security Awareness Training help local government?

Reduce Breaches and Infections

- Improve mindset and behavior
- Create a sense of shared security responsibility
- Reduce over-reliance on technology

Meet Regulatory Requirements

- Implement best data governance practices
- Meet compliance objectives
- Implement affordable cyber-insurance

High Return on Security Investment (ROSI)

- Fewer infections
- Lower clean-up/support costs
- Stronger security posture
- Higher productivity
- High security benefit vs. operational costs

Which regulatory agencies require training?

1. Financial services
2. Health care (HIPAA)
3. Retail (PCI)
4. Government
5. Energy (PUC)

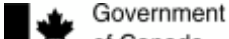














THE FULCRUM GROUP
One Technology Solution: Yours

What results should I expect from a training program?

Fewer infections and costs due to user error

Increased profitability, high ROI

Lower support costs, less time spent remediating

Empowered users who are now the first line of defense

Security-aware culture with measurable progress

Compliance with best practices and regulations

Cyber Threats - Phishing

- Generic Email Phishing
- Spear Phishing/Whaling
- Smishing and Vishing
- Business Email Compromise

Use the SLAM Method to Detect Phishing Emails

Sender

Check the sender closely. Look for misspelled domains, or a completely different email address than the name of the sender. Ultimately, if you don't recognize the sender, proceed cautiously and don't open attachments.

Links

Hover over (but don't click) on any links, and avoid clicking on any links that you don't recognize. You can also type in the URL of the site directly.

Attachment

Don't open attachments from anyone that you don't know, and be suspicious of attachments from people that you know, but weren't expecting.

Message

Check the subject line and body for suspicious language, misspelled words, and bad grammar.

Passwords Best Practices

- If your organization allows it, use a Password Manager
- Use passphrases instead of passwords
- Use unique passwords on every website
- Don’t store passwords in a file on your computer
- Longer passwords are better
- Check the Dark Web to see if your passwords have been stolen
- Use Multi-Factor Authentication when available

Working from Home

- Don’t connect a personal computer to the agency network
- Don’t access agency IT systems from a personal computer; only use agency computers to access agency IT systems
- Make sure your personal computers have up-to-date antivirus software and Windows updates
- Avoid Public WiFi connections when possible
- Don’t use any work passwords on personal web sites

Other Cybersecurity Tips

- Watch out for Social Engineering attempts
- Don’t connect your personal smart phone or tablet to the agency private WiFi; connect to the public WiFi instead
- Make sure your smart phone and any tablets have a passcode required to access
- Don’t plug in random USB drives to your agency computer (or personal computer)
- Lock your computer when you’re away
- Follow agency regulations on use of social media
- Only use agency-approved cloud applications

Q&A

> Any questions?

The Fulcrum Group, Inc.
1670 Keller Parkway
Suite 130
Keller, TX 76248

Phone: 817-337-0300
Help Desk: 817-898-1277
Web: www.fulcrum.pro
Support: helpdesk@fulcrumgroup.net