WELCOME TO

Uniform Network Security - Next Steps

PRESENTED BY:
Ed Knott - Applied Connective
Todd Lewis - Bytes Managed IT

Ed Knott

PRESIDENT

Applied Connective Technologies

- 20+ years in IT
- Offices in Albion, Columbus and Norfolk
- Managed Technology Provider
- Small/Medium Business
- Finance/Government/Healthcare

Todd Lewis

PRESIDENT

Bytes Managed IT

- 20+ years in IT
- Office in Scottsbluff
- Managed IT Services Provider
- Small/Medium Business
- Government/Healthcare

Uniform Network Security - Next Steps

Quick AGENDA

- The Human Factors of Cyber Risk
- Email Security and Threats
  - Phishing
  - Impersonation
  - Spear Phishing
  - Whaling
  - Spoofing
- Passwords and Management
- Multi-Factor Authentication (MFA)
  - Authenticator App
- Cyber Security Awareness Training (CSAT)

- 15 Ways to Protect Your County
- Handout / Document Review
- Backup Disaster Recovery
- Firewall and Perimeter Security
- Managed Endpoint Protection
- Monitoring and Patch Management
- Cable Plant and Network Infrastructure

The human factors of cyber risk

MAJOR CYBER RISKS		ROOT CAUSE
$6 trillion in 2021	Estimated cost of cyber attacks on organizations globally	**Organizations rarely invest in and plan for the human component of cyber security until after a breach has occurred. For major breaches, this can cost the organization millions of dollars.**
85%	of data breaches were attributed to human error or negligence	**Types of cyber threats and methods of prevention change each day. Instilling a culture of cyber interest and awareness equips an organization to better handle changing cyber security threats.**
47%	of IT professionals describe collaboration between security risk management and business as poor or nonexistent	**Many executives have the mindset that cyber security is the responsibility of IT; rather it is everyone's responsibility. Employee awareness should be the first line of defense for an organization's digital assets.**

Phishing

A phishing email is a scam or fraudulent attempt from a cyber criminal to trick the recipient into divulging sensitive information or clicking on a dangerous link or attachment to plant malware on your machine, infecting your system and potentially the entire network.

The cyber criminal typically poses as a trusted contact (coworker, family member, etc.), a business, or a well-known institution (UPS, Amazon, Microsoft, etc).

Phishing attacks are on a steep rise today—here are some stats to know!

3/4

organizations experienced a phishing attack in 2021

96%

are delivered via email

74%

of US organizations experienced a successful phishing attack last year

and the average cost of just one data breach is

$4.24M

More Email & Security Threats To Beware Of

Types of phishing

The difference between phishing, spear phishing and whaling attacks is on the scale of personalization. Phishing is the least personalized, whaling is the most, and spear phishing lies between.

Spear Phishing

The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

Whaling

Whale phishing is a term used to describe a phishing attack that is specifically aimed at executives, decision makers and others involved with management and finance. Because of their status, if such a user becomes the victim of a phishing attack he can be considered a “big phish,” or, alternately, a "whale."

Spoofing

Spoofing is a kind of attack where an untrustworthy or unknown form of communication is disguised as a legitimate source. Phishing often involves some kind of spoofing (whether email, website, caller ID, IP address, or DNS) to hide the true source of the attack and to make the attack seem more valid.

15 Ways To Protect Your County

This document is designed to be a quick assessment to identify tools and practices you should have in place to best position your organization to avoid cyber attack.

15 Ways To Protect Your County From A

Cyber Attack

Advanced Malware Protection
Prevent ransomware and other malware attacks with advanced endpoint security. Traditional antivirus has proven ineffective. Consider an advanced managed AI-driven solution monitored 24/7 by our SOC (security operations center). Don't just stop breaches—prevent them.

Email Security
Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce threats and your exposure to attacks on your staff via email.

Passwords
Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

Security Awareness
Train your users often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

DID YOU KNOW?

$4.2M is the average cost of a data breach today

74% of US organizations experienced a successful phishing attack last year

97% of breaches could've been prevented with today's technology.

Advanced EDR
Take your endpoint protection to another level. Endpoint Detection and Response (EDR) is your failsafe for threats that bypass firewall and endpoint security services. Discover known and unknown elements of an attack. Today's EDR solutions and services complement your advanced malware protection by protecting against file-less and script-based threats. EDR will reduce investigation and remediation time after an incident.

Multi-Factor Authentication
Utilize multi-factor authentication whenever you can, including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

Patch Management
Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

Dark Web Research
Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

SIEM/Log Management & SOC
(Security Incident & Event Management and Security Operations Center)
Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements. SOC is critical to monitor logs and events.

DNS Protection
Internet security is a race against time. Block malicious websites and filter out harmful or inappropriate content. DNS filtering ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks. Agent- or firewall-based coverage options should be considered.

Mobile Device Security
Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

Firewall
Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

Encryption
Whenever possible, the goal is to encrypt files at rest, in motion (think email), and especially on mobile devices.

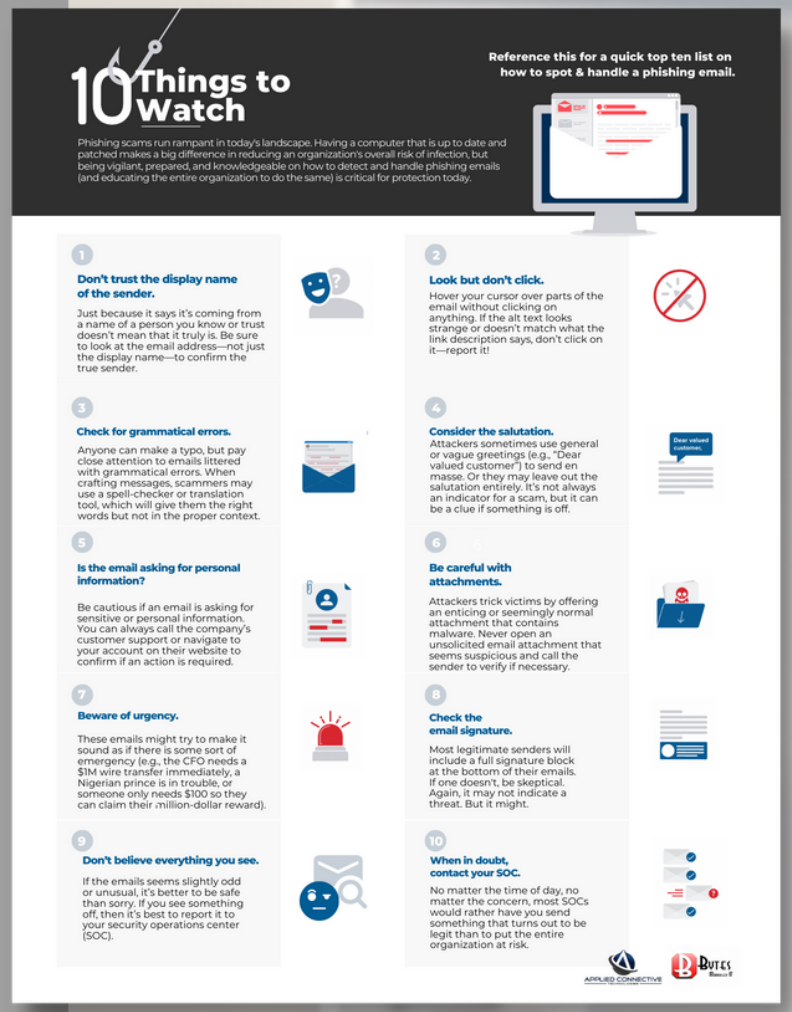
Backup
Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

Cyber Risk Assessment Not sure how to answer? Concerned about exposure? Get in touch with us.

Applied Connective | (866) 358-0109 | www.appliedconnective.com Bytes | (308) 635-2983 | www.bytesmanagedit.com

DOCUMENT REVIEW

Detecting A Phishing Em@il



10 Things to Watch

Reference this for a quick top ten list on how to spot & handle a phishing email.

Phishing scams run rampant in today's landscape. Having a computer that is up to date and patched makes a big difference in reducing an organization's overall risk of infection, but being vigilant, prepared, and knowledgeable on how to detect and handle phishing emails (and educating the entire organization to do the same) is critical for protection today.

1 Don't trust the display name of the sender.

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address—not just the display name—to confirm the true sender.

2 Look but don't click.

Hover your cursor over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it!

3 Check for grammatical errors.

Anyone can make a typo, but pay close attention to emails littered with grammatical errors. When crafting messages, scammers may use a spell-checker or translation tool, which will give them the right words but not in the proper context.

4 Consider the salutation.

Attackers sometimes use general or vague greetings (e.g., "Dear valued customer") to send en masse. Or they may leave out the salutation entirely. It's not always an indicator for a scam, but it can be a clue if something is off.

5 Is the email asking for personal information?

Be cautious if an email is asking for sensitive or personal information. You can always call the company's customer support or navigate to your account on their website to confirm if an action is required.

6 Be careful with attachments.

Attackers trick victims by offering an enticing or seemingly normal attachment that contains malware. Never open an unsolicited email attachment that seems suspicious and call the sender to verify if necessary.

7 Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer immediately, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

8 Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails. If one doesn't, be skeptical. Again, it may not indicate a threat. But it might.

9 Don't believe everything you see.

If the emails seems slightly odd or unusual, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).

10 When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the entire organization at risk.

This document can be used as a reference to help you identify potentially risky emails in your inbox.

DOCUMENT REVIEW

Top 4 Tips To Create Secure Passwords

1

Choose strong passwords

Each character you add to a password makes it more secure. Use passphrases! They are easier to remember and type than a random mix of symbols, letters, and numbers. **"I'm craving 4 ice-cream!"** vs **"z4t2)F3j*t6D3"**

2

Make them unique

Even the strongest password is insecure when used across different sites. If one gets compromised, all your other accounts will automatically be exposed.

3

Turn on MFA (multi-factor authentication)

When enabling a second factor of authentication, you add an extra layer of security to your accounts. You sign in with something you know (a password) and something you have (a code sent to your phone).

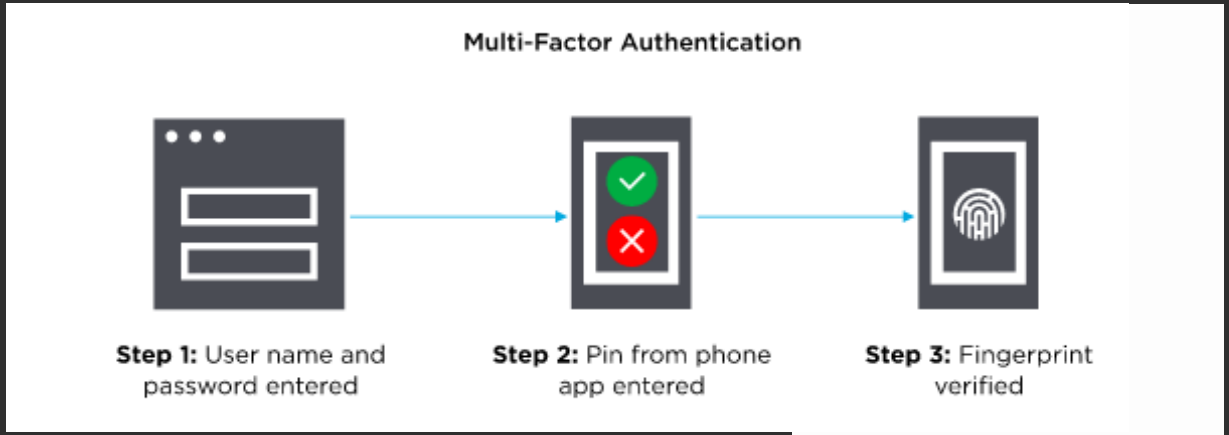
4

Use a password manager

Password managers are programs specifically designed to store and manage passwords securely. Instead of having to remember hundreds of strong, unique passwords, you'll only need to remember the master password to the encrypted vault.

What Is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.



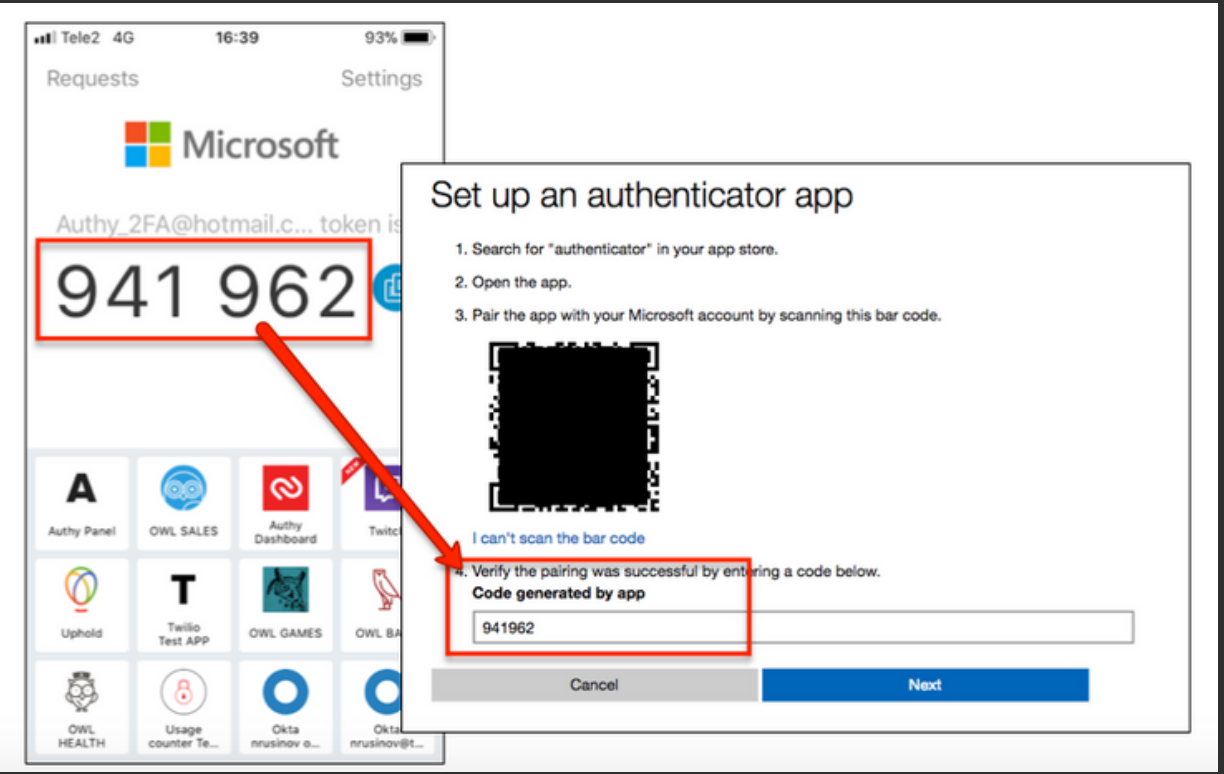
Most MFA authentication methodology is based on one of three types of additional information:

- Things you know (knowledge), such as a password or PIN
- Things you have (possession), such as a badge or smartphone
- Things you are (inherence), such as a biometric like fingerprints or voice recognition

Authenticator apps...why do I need one?

Authenticator apps generate a one-time code that you use to confirm that it's really you logging into a website or service; they provide the second part of your multi-factor authentication. Access to your authenticator app on your smart phone should be protected with facial recognition or biometrics for safety and ease of use.

- Using text message to retrieve your login code is less secure than using an authenticator app
- It's important to create a backup copy in case of device loss, theft, or any of the other unexpected turns that can take away your access
- SMS and call-based MFA is being phased out with vendors requiring authenticator apps or security keys



Cyber security risk assessment

Identify the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property) and understand the various risks that could affect those assets.

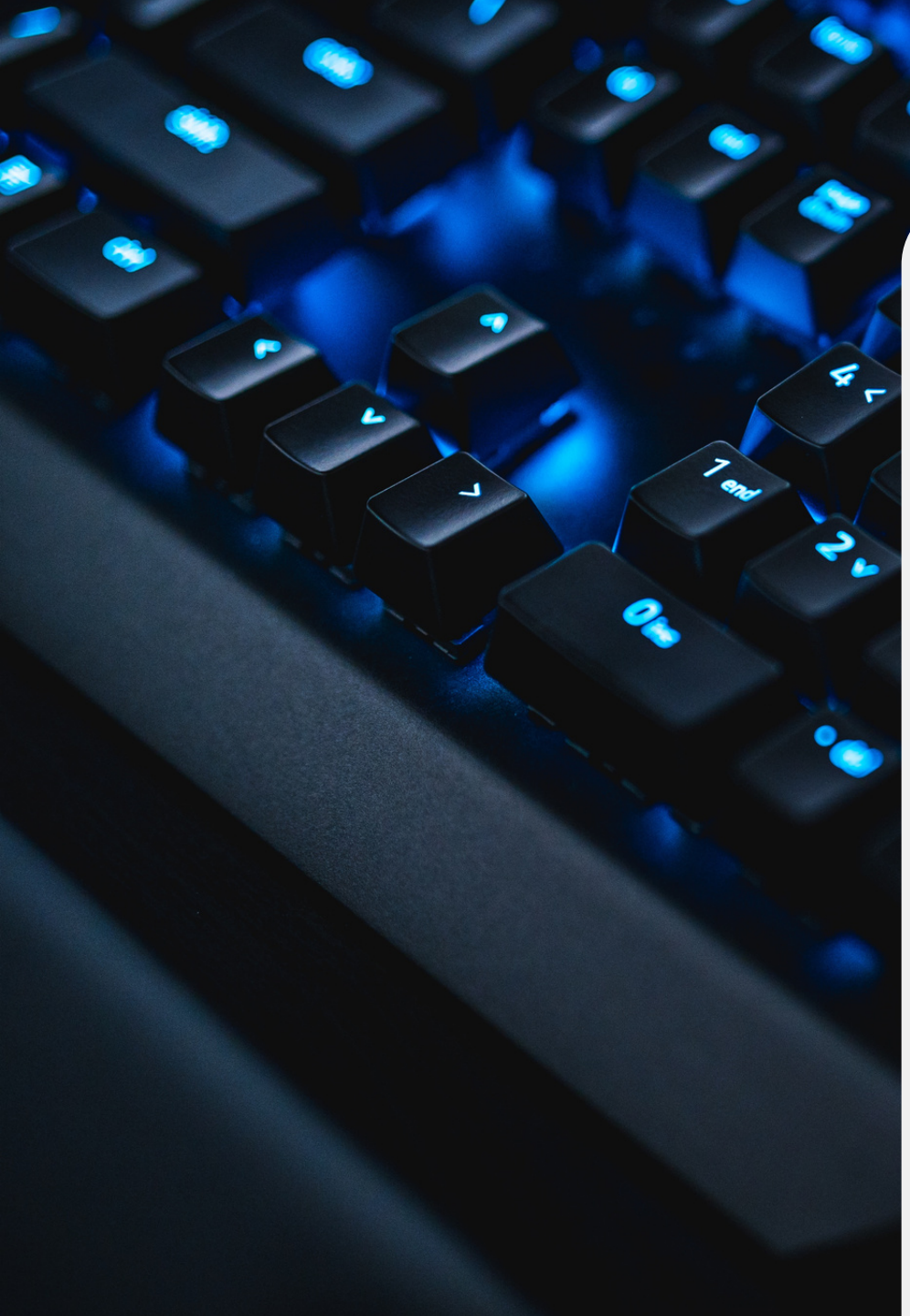
CISA Cyber Security Evaluation Tool

- Contributes to an organization's risk management & decision-making process
- Raises awareness & facilitates discussion on cyber security within the organization
- Highlights vulnerabilities in the organization's systems & provides recommendations on ways to address them
- Identifies areas of strength & best practices being followed in the organization
- Provides a method to systematically compare & monitor improvement in the cyber systems
- Provides a common industry-wide tool for assessing cyber systems

It's critical to understand the risks you face and know where you're vulnerable. The most effective way to do this is by partnering with a reputable IT company, who can conduct a thorough cyber security risk assessment, providing a comprehensive analysis and recommendations on mitigation, so you can make an informed decision on how you wish to proceed.

Knowledge is power. Leverage technology & your workforce to achieve optimal cyber security.

Q&A



Thank you for your time!

Ed Knott
(866) 358-0109
eknott@applieconnective.com
www.appliedconnective.com

Todd Lewis
tlewis@bytesmanagedit.com
(308) 635-2983
www.bytesmanagedit.com