



Ring in the New Year - Secure

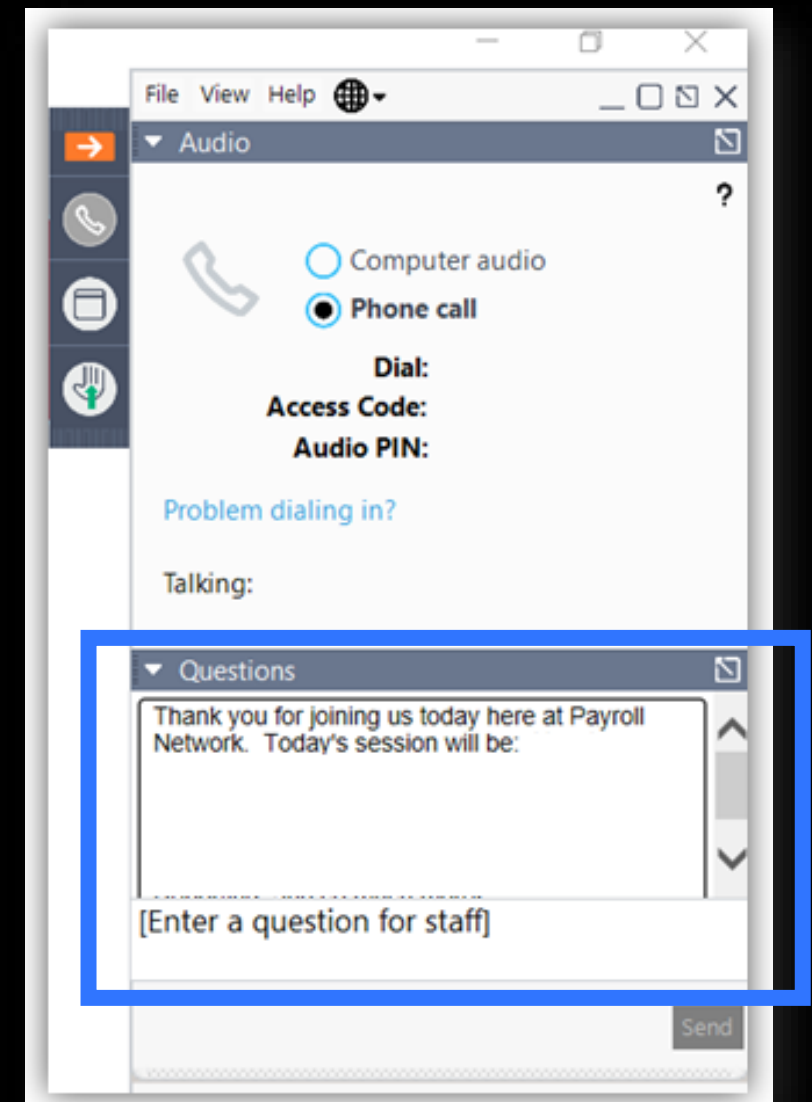
Cybersecurity Threats: Protecting Your Organization



- Webinar will be recorded
- All attendees will be placed on mute
- Ask questions!
- Survey will be sent after the webinar
- Handouts available
- Certified Course – polls!



For Today's Session





Legal Disclaimer

The information presented today is provided for educational purposes and should not be considered legal advice.

The presentation and these materials do not represent the opinions of the presenter and those of Payroll Network.

Your Presenter's Today



Amy Miller

- VP of Training
- Payroll Network/GovConPay



Nick Holcomb

- Chief Technology Officer
- Payroll Network/GovConPay

- Defining Cybersecurity
- Terminology
- Common Threats
- How to protect yourself


Agenda






Poll #1

Data Breaches exposed _____
records in 2021.



True Cybersecurity is
preparing for what's
next, not what was
last.



Neil Rerup
Cybersecurity Expert

Cybersecurity

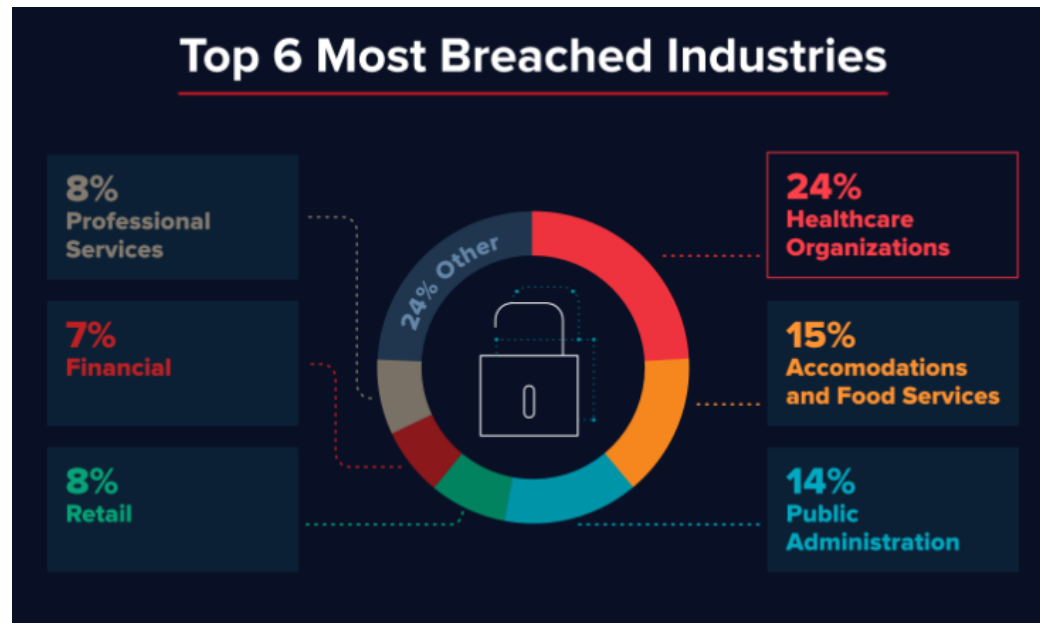
The practice of protecting critical systems and sensitive information from digital attacks.

Cybersecurity is a strategy that revolves around identification, protection, detection, response, and recovery.



Motives

- 90% of hacking is due to financial reasons or espionage
- Don't underestimate hackers' interest in your company
- Most people do not notice timely when their data has been compromised



Did You Know?

95 percent of cybersecurity breaches are caused by human error.

(World Economic Forum)





Poll #2

What size companies receive the highest number of malicious emails?

Terminology



Spoofing

- Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source – **such as your CEO or CFO.**
 - i.e altering the “From” field to match a trusted contact or mimicking the name and email address of a known contact.
- The goal of spoofing is to get you to **do something**, such as:
 - Changing **direct deposit** accounts to a fraudulent account.
 - Disclosing **confidential employee information** such as W-2s.



Spoofting

From: Charlie Wolf <admin@checkod.com>
Sent: Wednesday, January 3, 2019 2:18 PM
To: [REDACTED] <@payrollnetwork.com>
Subject: Direct Deposit

Hi

I want an update to be done on my DD information as I have change my bank. Can the change be effective for the current pay date?

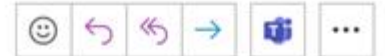
Regards

Charlie Wolf

Request for Year-end information



Amy Miller SHRM-CP, PHR
To: Amy Miller SHRM-CP, PHR



10:18 AM

Hello Amy – could you please send me a PDF of the W2 information for 2022 for my records?

Thank you.

Nick

[REDACTED]
Payroll Network, Inc. | 2092 Gaither Road, Rockville, MD 20850
(D)301.339.6011 | email: AMiller@payrollnetwork.com



Phishing

- Phishing is sending emails, messages, or linking to websites pretending to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- The goal of phishing is to get you unknowingly **share your password** with a malicious actor.

57 percent of organizations see weekly or daily phishing attempts.



Phishing

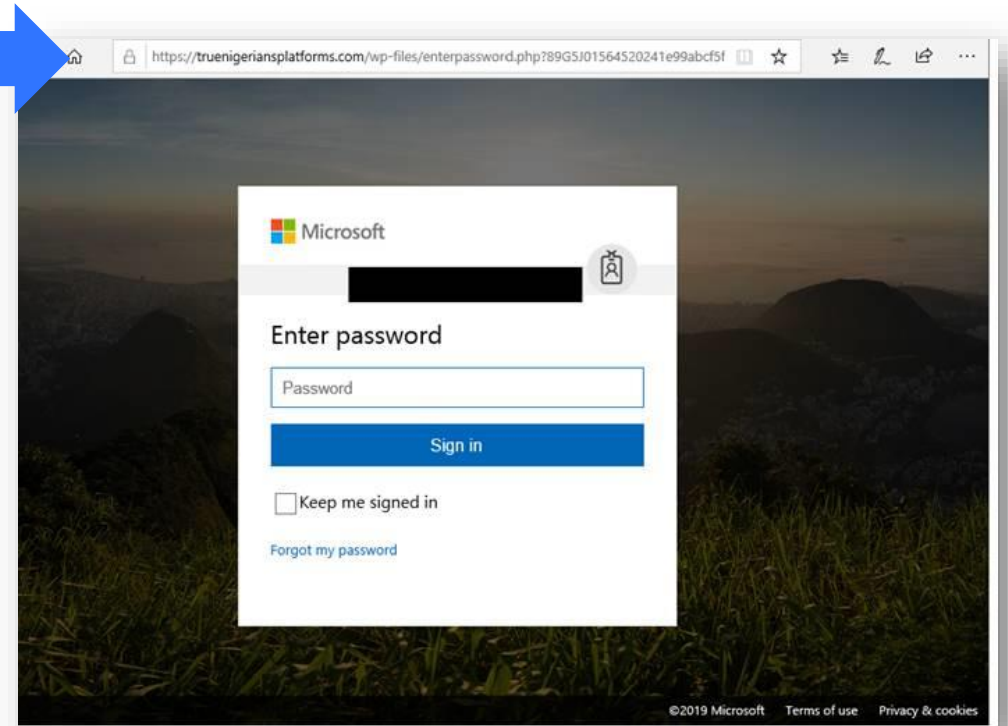
From: RingCentral_VMS IncomingCall Delivery Notifications For Mailbox (305)
<2ndxhyehrbbeuringcentral_calldwty132sh@hivestraeming.com>
Sent: Tuesday, July 30, 2019 3:19 PM

Subject: Incoming_RingCentral Call Received on 7/30/2019 at 1:18 PM
Importance: High

On Tuesday, July 30, 2019 This caller left you a VoIP_VNote
Full length: 40secs.

Memo: "Hey It's me Jerry can you return....."

[LISTEN](#)



- Redirects to fake login page

Compromised Account

Email

- A compromised email account means that a malicious actor (hacker) has access to a legitimate email account.
- Emails from the hacker will appear technically the same as legitimate emails from the user.
 - Watch for unusual language and misspellings.
- If your account is compromised, hackers could potentially:
 - Asked for **password resets** and credential changes.
 - Request **unauthorized direct deposit changes**.
 - Ask for **unauthorized** purchases.

Compromised Account

Email

I am sorry if this is going to be too much trouble , i am having trouble getting into isolved ,
did forget password and the security question answer is not it .

Please HELP reset .

Respectfully,

Director of Finance

Phishing and Spoofing – Best Practices

- Slow Down – evaluate your emails / links carefully
- Validate the sender – never open attachments from unknown senders
- Validate the URL
- Look for inconsistencies in the language
- Look for threats / scare tactics
- NEVER send / supply sensitive data or passwords
- Ensure a strong password (Pass Phrases vs. Passwords)
- Do not re-use old passwords
- Enable Multi-Factor Authentication



Multifactor Authentication


- MFA is a method of verifying who you are that requires the use of more than just a username and password.
- Users are required to acknowledge a phone call, text message, or app notification on their smart phones after correctly entering their passwords.
- They can sign in only after this second authentication factor has been satisfied.
- Notifications / require entry of code

This is built into registration process for ESS in isolved – supplying cellphone information.



@payrollnetwork.com

Enter code

 We texted your phone +X XXXXXXXX63. Please enter the code to sign in.

Code

☐ Don't ask again for 14 days

Having trouble? [Sign in another way](#)

[More information](#)

Verify



Have you been
PWNED?

Did You Know? Ransomware

In a 2022 survey, it was found nearly two in three midsize organizations have suffered a ransomware attack in the past 18 months. Even more concerning is that 20% of them spent at least **\$250,000** to recover from it.





Poll #3

Do you have a remote working / workers policy at your organization?

Remote Work

- Remote workers will continue to be a target for cybercriminals.
- Because of these remote workforces, cloud breaches will increase.
- Increase use of MS Teams (500%)
- Securing files continues to be an issue.

Tools

- Multi-factor Authentication
- Training / Policy Awareness
- VPNs
- Encryption
- Centralized Storage Solutions (Paperless Policy)
- Secure Wifi Passwords
- Endpoint Management
- Monitoring and Testing



How to Protect Yourself



What you need to do

- #1 – Are you holding regular Security Training?
- **Educate** individuals – Awareness is key
 - Show them what's in it for them
 - Make it clear no one is safe
 - Start the training from Day 1 – Onboarding
 - Train on a regular cadence – not one and done
 - Create a Cybersecurity Training Plan and make it available
 - Recognize and reward employees
 - Set the tone across the organization – not just at an employee level



What you need to do

- ✓ Put Policy into Practice
 - Do you have a Cybersecurity policy?
- ✓ Institute policies for example:
 - **Use iSolved**
 - **Call** the requestor
 - Never use email as the final word
- ✓ **Multi-Factor Authentication**
- ✓ Test your employees



Client Responsibilities

- Self Service access
 - Enable access at time of hire and encourage employees to use
 - Direct Deposit changes
 - Address changes
- Do not make changes to employee information based-on email alone
 - Use iSolved processes (Workflows / Forgot Password)
 - Voice confirmation

Important Payroll Safeguards

- Do not share accounts / logins to isolved
 - We can create individual logins with appropriate access
- Do not make changes from an email request
 - Take the time to make the call
- We will not update your data for you – unless Managed Services
 - Guidance on how to complete will be provided
- Keep your Security Contacts up to date
 - i.e Qtrly work with our team to review who has access and who can call on behalf of your company
- Ensure you have a Security Officer at your company on file with our team.

Processing Payroll – Watch List

- **Always review:**
 - New Employee and Change Audit report
 - Double check New Employees
 - Review Direct Deposit changes
 - Payroll Summary
 - Review totals
 - Payroll Register
 - Exceptions



Review - Best Practices

- Never provide sensitive personally identifiable information (PII) within an email.
 - Never respond to pop-ups or unsolicited phone calls asking you to provide personal information or to submit or re-submit your login and password information.
 - Review email and domain names closely for accuracy and to help avoid phishing or BEC schemes. Payroll Network emails will always follow the @payrollnetwork.com structure.
 - Validate every and all payment requests received via email – ideally verifying the sender's detail via phone call or in person before proceeding.
- Never allow multiple people to use the same computer to process a transaction.
 - Never continue an online session that makes you or any of your colleagues feel uncomfortable or unsure, discontinue the session immediately.
 - Regularly review and confirm the entitlements and systems access of your employees.



Poll #4

Do you have a business continuity plan?

**Continue to visit our
website for training/blog
posts/webinars, etc.**

payrollnetwork.com

support@payrollnetwork.com

hradvisor@payrollnetwork.com



*upgrade available

