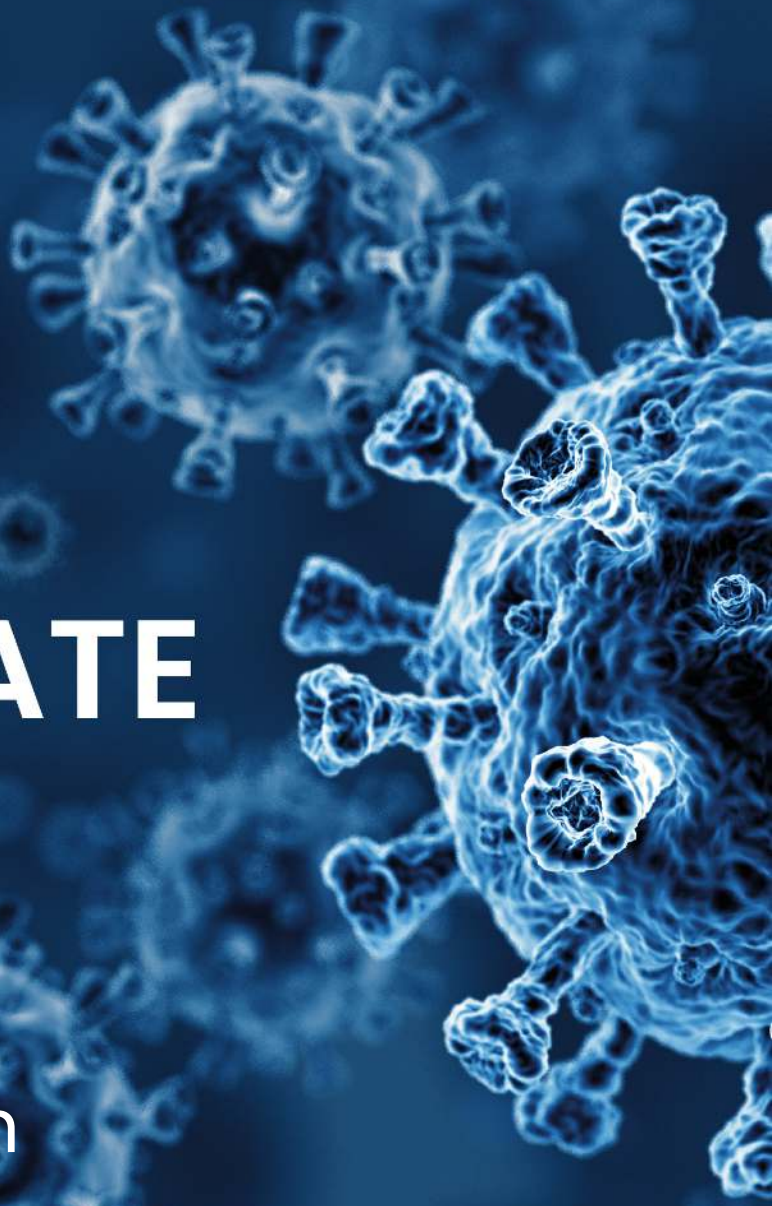
Payroll Network℠

COVID-19 UPDATE

April 16, 2020

Cybersecurity Threats: Protecting Your Organization in a COVID-19 World



For Today's Session

Payroll Network℠

- Webinar will be recorded
- All Attendees will be placed on mute
- Questions may be input into the Questions Box within the GOTOWEBINAR
- Survey will be sent after the webinar

Background – Nick Holcomb

Payroll Network℠

Chief Technology Officer

- 20 Years Technology Experience
- 15 Years Industry Experience
  - Payroll | Talent | Time | HR | Compliance
  - Reporting | Application Integration | Mobile
  - Executive Leadership
- Certifications: Microsoft Certified Professional
- B.A. American University

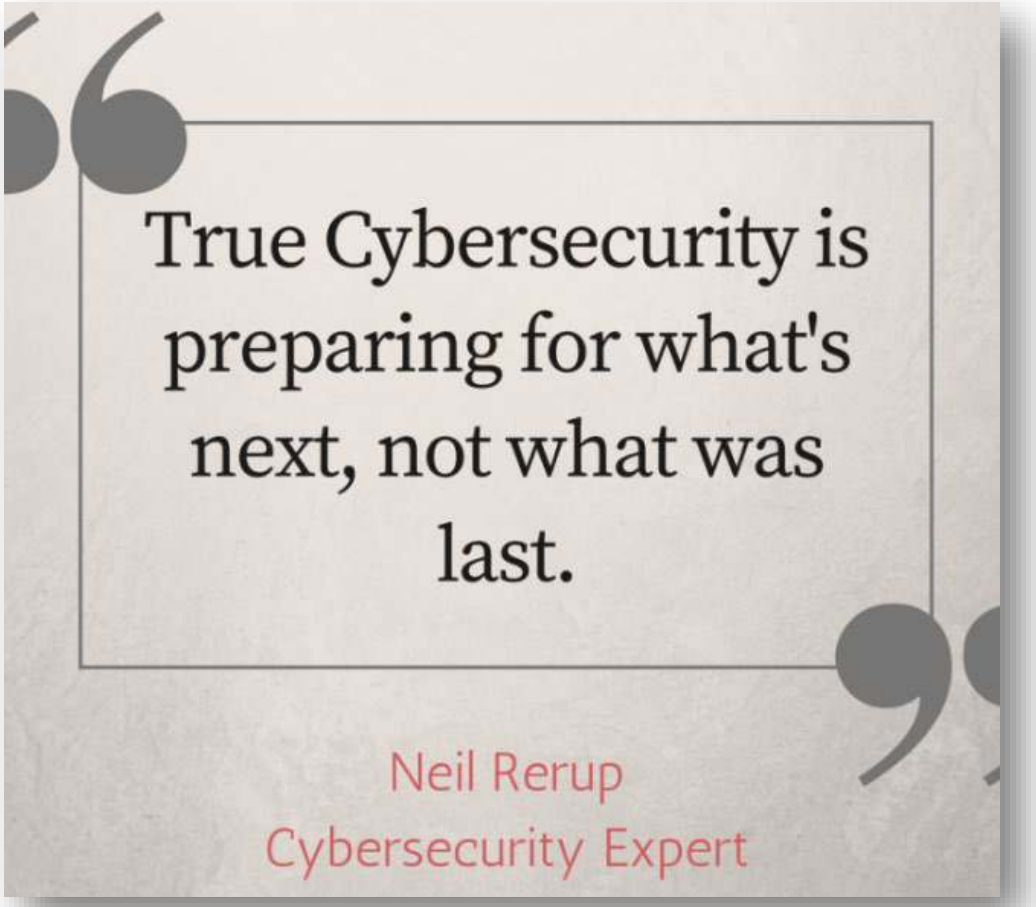
Agenda

Payroll Network℠

Cybersecurity in a COVID-19 World

- Cybersecurity Strategy - 8 Key Factors
- Avoiding Coronavirus Scams
- Beware of Phishing and Email Fraud
- Protecting a Dispersed Workplace
- Payroll Reminders

Payroll Network℠



Kaizen

Payroll Network℠

Continuous Improvement

- You must continually improve your cybersecurity strategies
- If you are doing the same thing as a year ago, you are doing something wrong

IT Protection Components

Payroll Network℠

Eight Components of an IT Protection Strategy

1. Web Filtering
   - Incoming email filters
   - Content filtering with DNS tools
2. Perimeter Security
   - Physical firewall hardware
3. Access Control
   - Password policies
   - Multi Factor Authentication (MFA)
   - Personally Identifiable Information (PII)

IT Protection Components

Payroll Network℠

Eight Components of an IT Protection Strategy

4. Data Encryption
   - At-rest (database)
   - In-transit
5. Endpoint Device Protection
   - Antivirus
   - Malware remediation tools

IT Protection Components

Payroll Network℠

Eight Components of an IT Protection Strategy

6. Patching Policies
   - Windows Updates
   - Sunsetting legacy systems
7. Backup & Recovery
   - Onsite/offsite/cloud
   - Periodic testing
8. User Education / Security Awareness Training
   - Email threats
   - Targeting individuals with fiduciary responsibilities

Email Threats

Payroll Network℠

Evolving Trends

- Email attacks previously took the form of worms and viruses, which would attempt to deploy harmful software to a users' PCs and then spread rapidly across the local network.
- Today, the objective of most email attacks is to commit fraud – **actual theft of money**.

Phishing

Payroll Network℠

What is Phishing?

- Phishing is an email posing as a valid cloud service (such as voicemail, file storage, etc.) and attempting to have you login to a fake site.
- The goal of phishing is to get you unknowingly **share your password** with a malicious actor.

Spoofing

Payroll Network℠

What is 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.**
- 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.

Email Threats

Payroll Network℠

Coronavirus

- Cybercriminals send emails claiming to be from legitimate organizations with information about the coronavirus:
  - Emails designed to look like they're from the U.S. Centers for Disease Control or World Health Organization
  - Emails offering medical advice to help protect you against the coronavirus
  - Emails targeted employees' workplace email accounts on policies

Phone Threats

Payroll Network℠

Tips from the FCC

- Do not respond to calls or texts from unknown numbers, or any others that appear suspicious.
- Never share your personal or financial information via email, text messages, or over the phone.
- Be cautious if you're being pressured to share any information or make a payment immediately.

Phone Threats

Payroll Network℠

More Tips from the FCC

- Scammers often spoof phone numbers to trick you into answering or responding. Remember that government agencies will never call you to ask for personal information or money.
- Do not click any links in a text message. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they weren't hacked.
- Always check on a charity (for example, by calling or looking at its actual website) before donating.

Dispersed Workplace

Payroll Network℠

Security Challenges for Remote Workforce

- Remote access security
  - VPN vs Cloud-based
- "Shadow IT": using personal equipment for work
  - Eight Components of IT Protection Strategy
  - Scams may be harder for end-users to detect if using mobile devices or other personal equipment

Dispersed Workplace

Payroll Network℠

Security Challenges for Remote Workforce

- Meeting software security
  - Prevent “Zoom-bombing” by changing default screenshare settings and adding a meeting password
  - Chat over-share: remind your employees of proper chat etiquette

What you need to do

Payroll Network℠

How to protect your organization

- **Educate** individuals
- Institute policies for example:
  - **Use HCM** workflows
  - **Call** the requestor
- **Multi-Factor Authentication**

Client Responsibilities

Payroll Network℠

Payroll Watchlist – Employee Information

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

Client Responsibilities

Payroll Network℠

Payroll Watchlist – Payroll Processing

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

Client Responsibilities

Payroll Watchlist – Payroll Processing

- ACH and Banking Confirmation

Questions?

Additional IT Guidance

Payroll Network℠

Resources

Resources for Small Businesses

- https://www.computershowcase.com/category/resources

Coronavirus Guidance from Federal Agencies

- https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people
- https://www.fcc.gov/covid-scams

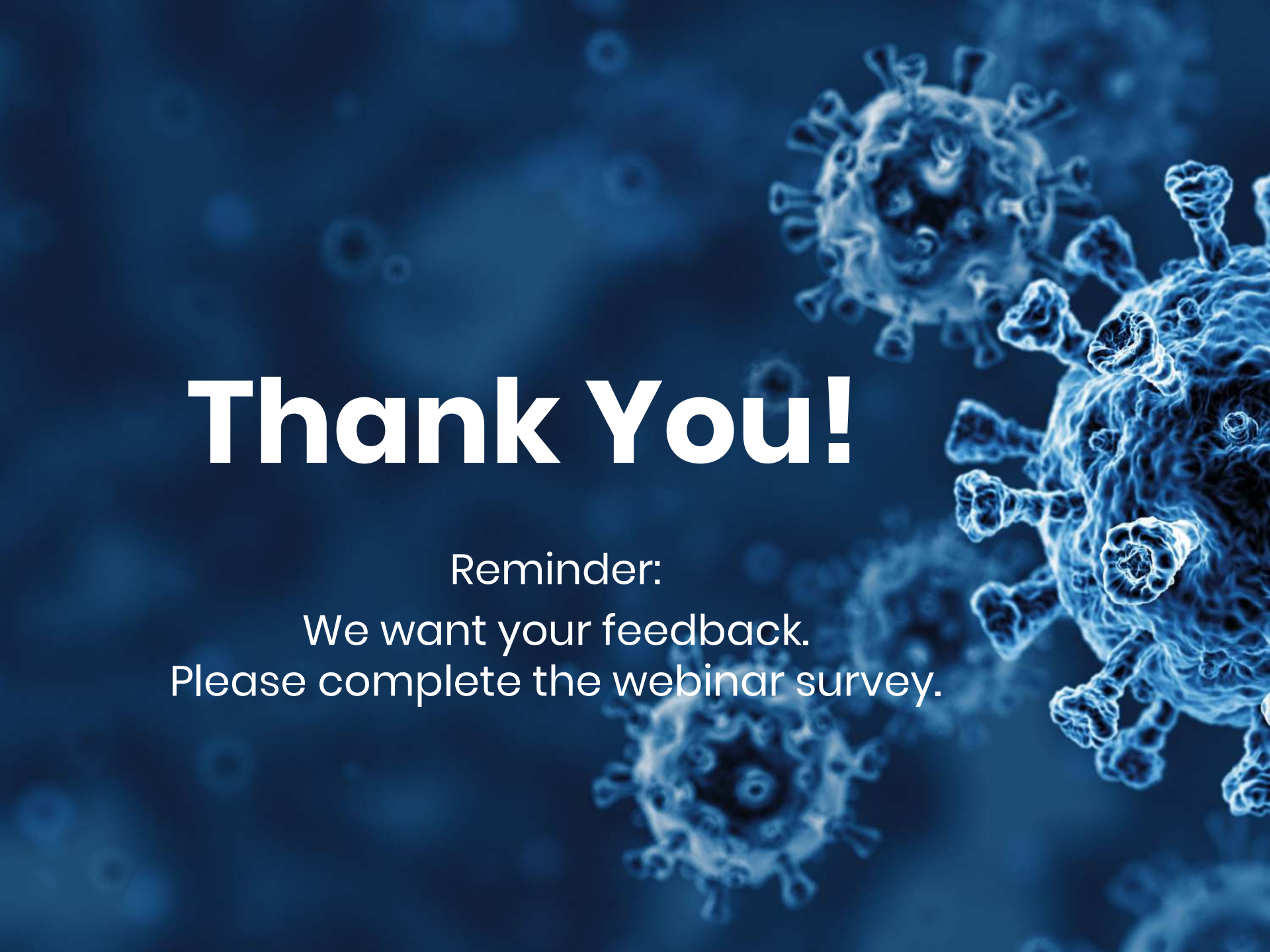
Contact Us

Payroll Network℠

Any Questions?

Please email:
support@payrollnetwork.com

Or call:
301-339-6000


Thank You!
Reminder:
We want your feedback.
Please complete the webinar survey.