April 19 - 21

NNAHRA

NATIONAL NATIVE AMERICAN HUMAN RESOURCES ASSOCIATION

25th Annual Conference

Honolulu, Hawaii

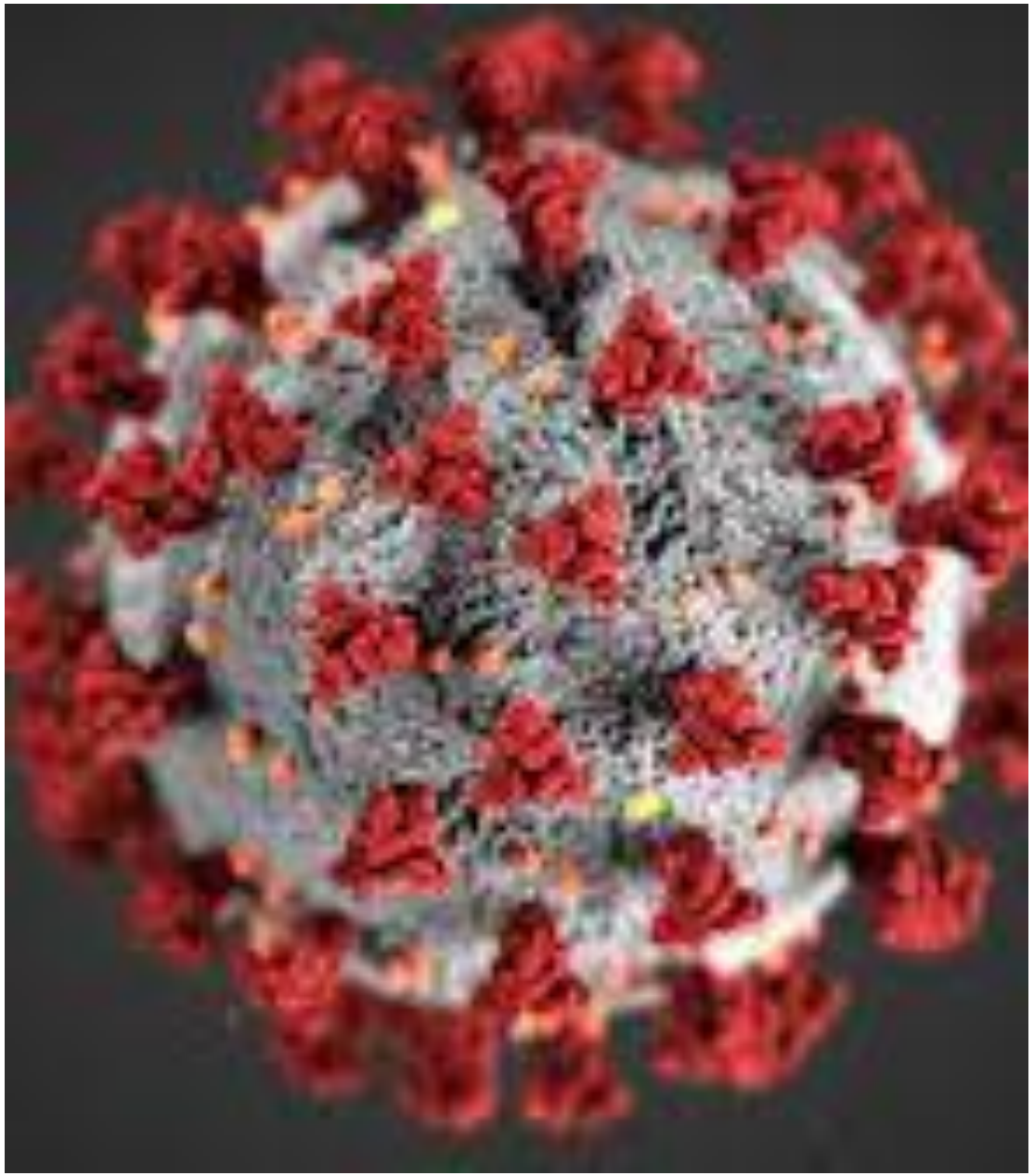
REDUCING RISK POST COVID: EMPLOYEE SAFETY AND CYBER SECURITY

Delane Big Crow, AINS, NFPA CFI-I

AMERIND Safety Services Manager

INTRODUCTION

COVID changed our workplaces in many ways. Today we will go over COVID and the effects it has had on Workplace Employee Safety, Cyber Security and the risks we face as we emerge from the Pandemic.



WORKPLACE AND EMPLOYEE SAFETY/RISKS

Workplace safety plans, remote work, vaccine mandates, COVID testing

WORKPLACE SAFETY PLANS

- 42% Lack of workplace safety policies, 9/10 Tribal entities did not have a Infectious Control/ BBP Plan prior to pandemic
- Lack of knowledge to create or update policies pertaining to Infectious Diseases
- 7/10 Tribal entities exceeded CDC guidelines during pandemic

REMOTE WORK

- Increase of remote work or hybrid working due to pandemic
- Working from home, Increase or decrease in productivity?
- Cyber security breaches with the increase of remote and online work options

VACCINATION POLICIES

- 4 out of 5 Tribal entities visited required Vaccination proof for visitors and employees on site
- Vaccines provided by Tribal Health
- Policies developed by Tribes for employees to receive vaccine as work requirement

COVID TESTING REQUIREMENTS

- Require periodic testing for employees to work in the office
- Require testing after contact with COVID positive or travel
- Mask mandates in office?

EMPLOYEE MENTAL HEALTH

- Increase in mental health issues during pandemic. Employees spending more time at home, out of routine, new burdens or responsibilities arise
- What programs are offered by tribal communities to battle the arising mental health crisis?

CYBER SECURITY

Cyber attacks and identifying the various types

WHAT IS RANSOMWARE?

- A malware that encrypts and locks a user out of their computer or device.
- Hackers usually go after sensitive data and information.
- Hackers use this malware to get a user to pay some sort of ransom to get their information back.
- How do these attacks happen?

PHISHING ATTACKS: WHAT TO IDENTIFY

- Again, ransomware is malware that attacks a system through what is called phishing.
- Phishing happens when hackers send a fake e-mail or corrupted link to a user.
- Once the user clicks on the link the malware will begin to encrypt and lock any data files it can.
- After all data on that system is encrypted and locked a screen will appear asking to the ransom!

SHOW ME THE MONEY!!!

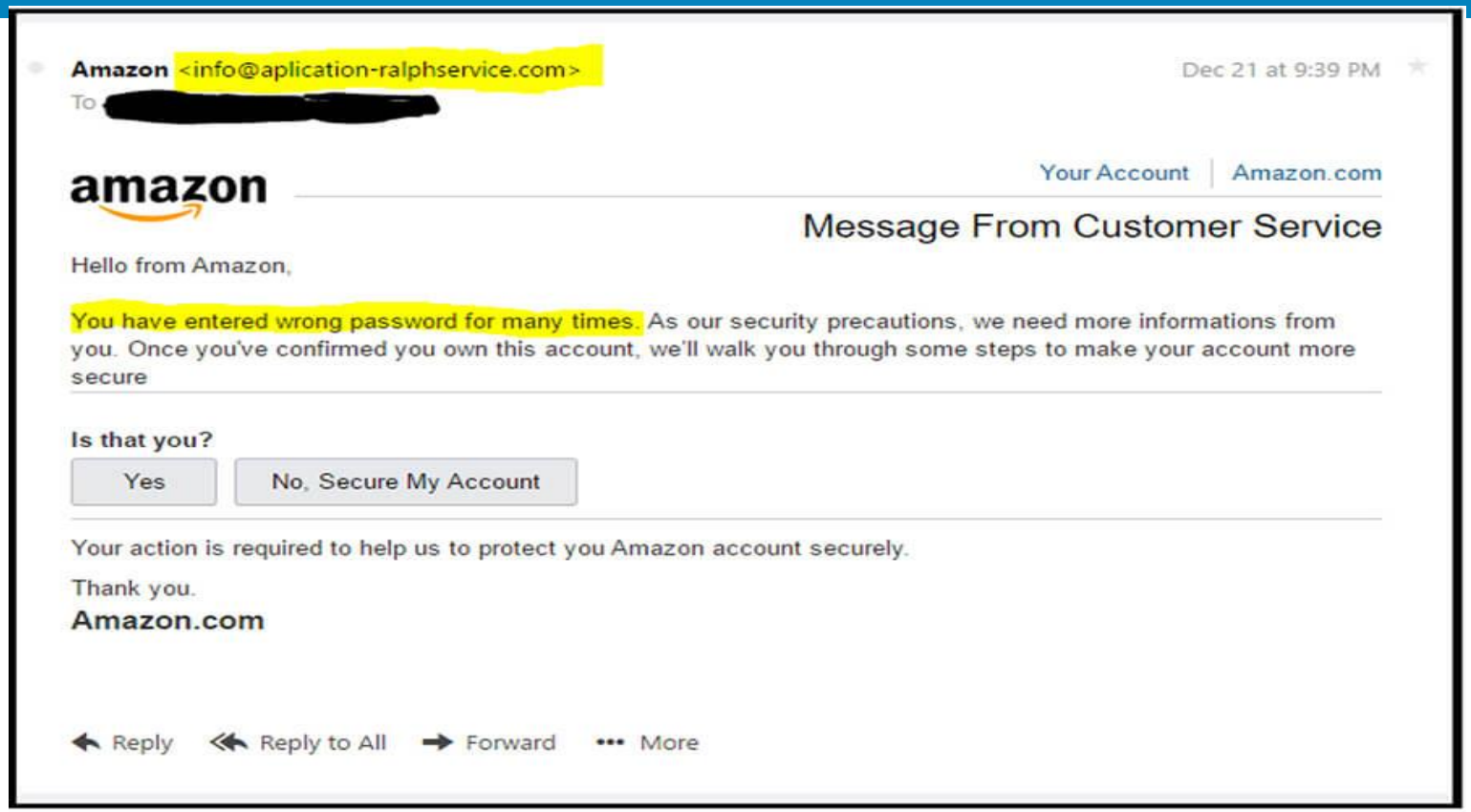
INFORMATION = VALUABLE

- Ransomware is very effective because information is very valuable.
- Ransomware is a low risk attack method for cyber criminals due to online currency such as Bitcoin.
- Bitcoin allows cyber criminals to receive payment and remain completely anonymous.

WHO IS AT RISK?

- EVERYONE!!
- Cyber criminals see personal data and sensitive information as $$$.
- Ransomware is effective because everyone needs access to their information.
- Be aware of suspicious e-mails and the URLs that are attached.

EXAMPLES OF WHAT TO LOOK FOR!



Amazon <info@aplication-ralphservice.com> Dec 21 at 9:39 PM

To [redacted]

amazon

Your Account | Amazon.com

Message From Customer Service

Hello from Amazon,

You have entered wrong password for many times. As our security precautions, we need more informations from you. Once you've confirmed you own this account, we'll walk you through some steps to make your account more secure

Is that you?

Yes | No, Secure My Account

Your action is required to help us to protect you Amazon account securely.

Thank you.

Amazon.com

Reply | Reply to All | Forward | More

ANOTHER EXAMPLE

Reply Reply All Forward

Thu 19/05/2016 2:10 PM

Peter Marshal <pchapman43@cox.net>

Robert Epps - Fiscal Return Letter AU/11260

To Robert@epsoft.com.au

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Message Robert Epps.doc (184 KB)

Australian Taxation Office - 05/19/2016
for Robert Epps

Fiscal Refund Notification

We have examined your tax report for the preceding quarter and concluded that you are qualified for a repayment of 746.27 AUD which is your accumulated tax excess. Please fill-out and return to us the attached tax repayment form, allow seven working days.

Note that the refund can be delayed for multiple reasons:

1. Applying after declared deadline
2. Provision of erroneous or incomplete data

BE AWARE OF WHAT IS BEING SENT TO YOU

- “You’re a winner click to claim your free gift card”
- Cyber Criminals also will send fake bank e-mail requests. Always log on through the banks home website.
- When you are suspicious about an e-mail link, hover over the link to see if it matches the sender or URL.
- Always use caution when receiving “weird” e-mails.
- Remember Cyber Criminals have thought about multiple ways to trick you.

ALWAYS BE CAUTIOUS

BEWARE OF SUSPICIOUS LINKS AND ATTACHMENTS.

Do not click on links or download attachments from unknown sources.

Do not install any applications from unknown sources.

Beware of suspicious links and attachments. They could be malware.

What is Malware?
Malware is a malicious software which, once downloaded, attacks and infects your devices.

SYNCLATURE
Mitigating Business Risk

SPEAR PHISHING

- Cyber Criminals know what they want and will do anything to get the information they want.
- Attackers will do their “homework” and know your contacts, work schedule and even your hobbies.
- Social Media plays a key roll in this type of attack.
- Once they have their information, their messages or e-mails will seem more legit.

SPEAR PHISHING

- Urgency: Gives you a deadline (respond soon or your account will be frozen)
- Authority: Pretends to be CEO, Colleague or trusted source.
- Mimic: E-mails imitating invoices or expense reports.
- Curiosity: Pretending to be HR

THE IMPACT OF SPEAR FISHING

- Financial Impact – Another way for Cyber Criminals to collect ransom.
- Sensitive Information and personal data lost.
- Impacts a users equipment and then can lead to IT problems.
- Can not only impact your personal life but can be devastating for a company as well.

BE AWARE BE SAFE!!

- Remember, be aware of suspicious e-mails.
- If it seems too good to be true it probably is.
- Cyber Criminals have been phishing for years and have probably thought every scenario. Stay Safe and use extra caution!!

QUESTIONS?

AMERIND

Insure Confidently

THANK YOU

Delane Big Crow dbigcrow@amerind.com www.amerind.com

NNAHRA

NATIONAL NATIVE AMERICAN HUMAN RESOURCES ASSOCIATION