

A Qualitative Study of the Trucking Industry's Phishing Awareness Training Method



Jonathan Dalia

IT Director,

Langer Transport

One Click

- October 23, 2018
- Invoice.pdf
- The entire server farm was encrypted
- Servers were blown away from the VMware cluster from 30,000 feet
- Every Server was restored from backup over the next 5 days

Timeline

- Monday 7:00 AM Wake up
- Monday night/ Tuesday morning, 12:15 AM – About to go to bed, and the phone rings
- No systems are accessible
- Ransomware note discovered
- 1:30 AM – flight booked to NJ and bags getting packed.

Timeline cont.

- 10:00 AM Tuesday flight arrived at Newark Airport
- Work on restoring systems. The backup system was overloaded, so the restore took a while and was slow.
- 11:00 AM on Wednesday, I had to stop due to exhaustion.
- Over the next 5 days, every server was brought back online, properly cleaned, and sanitized.

Is Phishing still an issue?

Current Headlines

- Over 2B users face phishing risks after Google data leak.
- AI-powered phishing attacks are on the rise and getting smarter
 - Generative AI is blurring the lines of reality.
- Don't fall victim to the new 'billion dollar' hack, federal agents warn
 - Pretexting is being used more heavily to build trust
- Warning for Windows Users: Global UpCrypter Phishing Attack is Expanding
 - Hackers are using fake voicemails and purchase orders to spread UpCrypter malware, giving them remote control over Windows systems worldwide.

Security Awareness Training

- Necessary for today's communications.
- Helps strengthen the weakest link in the security chain of the organization.
- With generative AI and other emerging technologies, the challenges facing users and security administrators are constantly growing.

Security Awareness Training

- Security Awareness Training is not a science and does not have extensive research behind it.
- This was a qualitative study done to understand the challenges from the user's perspective.
- Some valuable feedback was obtained.

An opportunity for research

- Challenges

- Many different learning styles are using a single platform to learn.
- Many users don't fully understand why they need to be trained.
 - The users usually know that hackers will get in, but they don't always understand that clicking a link can start a chain reaction that can paralyze a company.
- Live Interaction is usually not available for users.
- Teaching users to scrutinize all communications before proceeding is challenging, especially in the trucking industry, where communication can move a mile a minute.

Recommendations

- Perform the security training in groups where a member of the company's security team can be available to answer questions.

Recommendations

- Use dynamic testing to focus on the areas that need to be strengthened on a per-user basis.

Recommendations

- Explain to users why Security Awareness Training is important to this organization and to the end user.
 - If users feel they are part of the solution and understand the necessity and their role, it is likely that they will engage more.

Conclusion

Thank you for attending

Are there any questions?