Don’t Click: Title Agency Training Key to Preventing Phishing Scams, Other Cyber Attacks

By David Tandy
President, Texas National Title
TLTA Cyber Security Advisory Group
Feb. 23, 2021

The FBI reports a fourfold increase in cybersecurity complaints since the beginning of the pandemic, and cybercrime losses exceeded $1 trillion in 2020. Phishing emails, which trick recipients into clicking malicious links, remain one of the most popular forms of attack.

The title industry has increasingly become a target of cyber threats and those attacks, especially phishing emails, have become more sophisticated. Employees working remotely have further increased companies’ vulnerability by working from computers that are not as well-protected as computers at company offices.

It's difficult for today's title agency owners and management to know where to start or how much to invest in increased cyber security. But you should be aware that a company’s biggest vulnerabilities require more will power than financial investment. According to the SANS Institute, spear phishing attacks account for 95% of the breaches in enterprise networks. Therefore, if you want to greatly decrease your company's vulnerability to cyber attacks, training employees to recognize and report malicious links is among your most effective means to avoid falling victim to email phishing attacks.

As these types of phishing attacks become more sophisticated, they do an increasingly better job of creating a sense of urgency (or a sense of trust) that tricks recipients into an "autopilot mode". They see an email in their inboxes carefully worded to where they click on the link that then downloads malicious software into a company's computer system. Below are some recent examples of attacks I’ve seen carefully worded to crease urgency or trust:

From: System Software texasnationaltitle.com <secure@authentisign.com>
Sent: Thursday, October 22, 2020 6:18:52 AM
To: David Tandy
Subject: david.tandy 10/22/2020 7:18:51 a.m.

From: rusty
Sent: Monday, November 30, 2020 11:12 AM
To: David Tandy
Subject: [redacted] Corey - Payoff 3.xlsx

Adobe Online Attachments Expires Dec 30, 2020

MX-4111N_20201119_081412.pdf 268.6 KB

Download Attachments

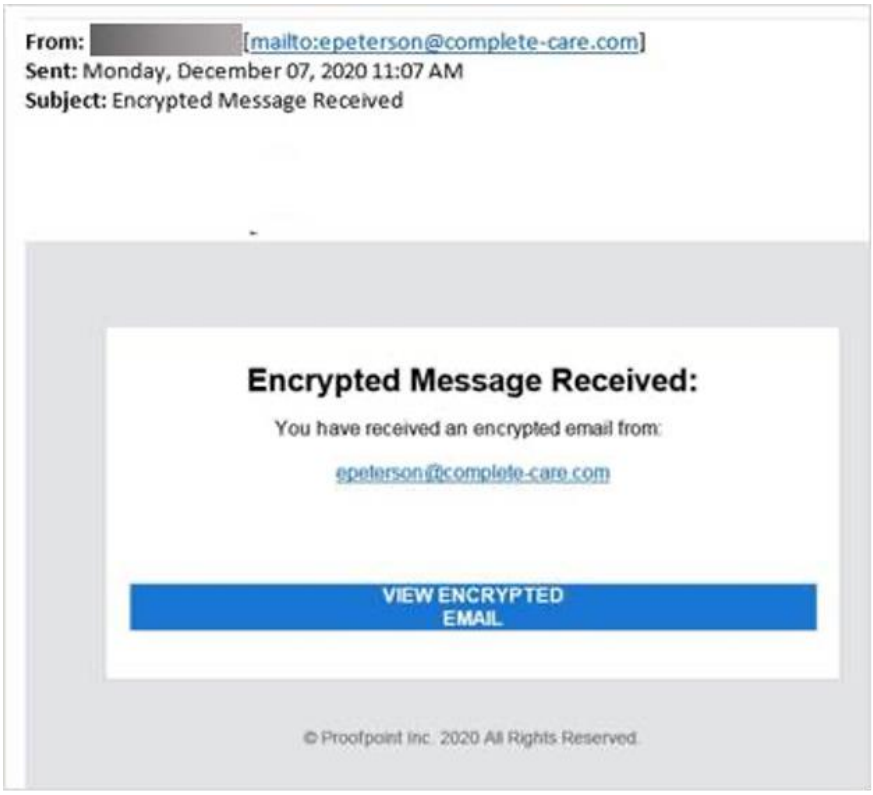
Rusty uses Adobe Online services to share documents securely. This message was intended for

Hello,

Here is the Payoff on Corey [redacted].

Thanks,

BEWARE OF CYBER-FRAUD Before wiring any funds, call the intended recipient at a number you know is valid to confirm the instructions - and be very wary of any request to change wire instructions you already received.



Phishing emails are carefully designed by criminals to manipulate our emotions and tap into our unconscious biases. By appealing to our biases and emotions, phishing tries to get us to make a fast rather than a thoughtful decision – and click the link. An email claiming to be from IRS, for example, takes advantage of the fact that people tend to obey orders given by authority figures, for example. Or, relying on a bias called "reciprocity," scammers might email what appear to be coupons from a reputable local retailer, and ask recipients to click on a button to sign up for the retailer's newsletter, relying on our natural inclination to pay others back in some way when we get a gift or freebie. Or as demonstrated in the examples pictured above, users can be tricked into clicking on a link because they are used to following instructions from their IT department, responding to lenders, etc.

It's not sufficient to simply warn employees about the ways in which that can be tricked by phishing attacks. Companies need to go further by testing employees throughout the year. For example, you could send simulated phishing emails and provide feedback to employees regarding their ability to recognize typical phishing emails that they should avoid and report as possibly malicious. There are a number of companies that provide "ready to go" and affordable training programs that include employee testing and tracking of results.

Although there are other ways for criminals to attack a company's computers with the goal of stealing data or damaging systems, by far the easiest and most popular method of attack

among cyber criminals is distributing mass numbers of phishing emails and wait for someone to do the work for them by clicking on a link that opens the door to cyber attack.