URGENT CYBER BULLETIN – SOCIAL ENGINEERING SCAMS

TO: U.S. RETAIL INSURANCE AGENTS & BROKERS
FROM: STEVE ROBINSON, RISK PLACEMENT SERVICE'S NATIONAL CYBER PRACTICE LEADER
RE: RECENT ALARMING INCREASE IN SOCIAL ENGINEERING SCAMS
DATE: September 10, 2020

In our continued efforts to educate our retail insurance agent partners and their insureds about the constantly developing cyber threat landscape, we want you to know about a real-time, concerning development. During the past 60-90 days, our cyber practice group has witnessed an increase in social engineering, wire fraud and payroll scams. Please share this information with your insureds in an effort to manage the risk of becoming a victim to these highly preventable crimes.

What is Social Engineering?
Simply put, social engineering is a tactic employed by criminals that uses human interaction in an effort to illegally obtain information about an organization or its digital assets. Often times, social engineering scams are designed to re-direct funds from an individual or company, unknowingly, to the criminal's bank account, instead of to the legitimate account for which the payment was intended. Social engineering tactics can also be used in an effort to gain access to network credentials or other information to allow the criminal to further carry out their crimes, undetected.

What Are We Seeing Specifically?
With relaxed controls, likely due to the work-from-home environment, we have seen a dramatic increase in fraudulent emails, purportedly from vendors, contractors, customers, or even employees alerting our insureds to any number of things, including:

- Change of corporate bank accounts/routing numbers
- Change in payment process from check to ACH
- Change in direct deposit information
- Soliciting sensitive information such as network credentials, passwords, etc.

For example, last month, one of our insureds received an urgent request, appearing to be from a contractor with whom they regularly do business. The contractor advised the insured that their payment process had switched from manual checks to ACH. The insured exchanged numerous emails with the bad actor and eventually issued two payments totaling more than $500,000 that the legitimate contractor never received.

Signs to Look Out For
There are numerous things to look out for to help recognize crimes of this nature. Here are just a few:

- Suspicious email addresses – check the URL, does it match the one you are familiar with? Generic greetings and signature – bad actors will try to adapt their communications to fit the broadest audience possible.
- Spoofed hyperlinks and websites – hovering over the hyperlinks may reveal URL's that don't match the text in the email.
- A sense of urgency when it should not be warranted.
- Requests to click on a link, visit a website, provide login credentials, process an invoice, change banking or payroll information or buy gift cards.

Prevention Tips

- Always verify the email request by calling the known number of the requestor on file (not the number provided in the email).
- If the sender requesting money or login credentials is unknown to you, do not respond and alert your internal IT personnel.
- Do not open attachments, click on embedded links or respond to emails that look suspicious or have any of the "Signs to Look Out For" characteristics listed above.
- There are many software solutions designed to scan inbound email for red flags of social engineering.
- Administer employee training to help employees recognize the signs and significantly lower your chances of becoming a victim.

Social Engineering Information, Articles and Training Resources

- U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency: https://us-cert.cisa.gov/ncas/tips/ST04-014
- NIST – National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. See page 40/80, Section 5.3 "Social Engineering"
- KnowBe4: https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees
- FBI – While this video addresses political campaigns specifically, there are great tips for avoiding social engineering scams: https://www.fbi.gov/video-repository/protected-voices-social-engineering-083018.mp4/view
- Forbes: https://www.forbes.com/sites/forbestechcouncil/2020/08/11/not-just-phishing-with-a-p-anymore-examining-the-a-to-z-of-social-engineering-attacks/#1603ae733168
- Norton: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
- Click "Learn More" after logging in to the RPS eCommerce Platform for access to discounts on phishing simulations and employee training: www.RPSSmallBusiness.com

###