Patriot Insurance Presents Anti-Phishing Tips Following NAIC Phishing Scam Report

Cyber security breaches are a very real threat, and they're on the rise. This means that the question is no longer if one will happen, but when. While the insurance industry is adept at helping families and businesses mitigate these types of risks, that doesn't mean that we're not susceptible to them too.

In a recent announcement, the National Association of Insurance Commissioners (NAIC) warned that agents and producers have been the target of a phishing scam, where hackers have posed as insurance regulators and sent fraudulent emails regarding a falsified claim related to their company that has been submitted to the NAIC. The email contains a call-to-action to click on a link to download the complaint notification, even using the NAIC and CIPR logos and originating from "naic" or gmail accounts, in an attempt to steal personal and confidential information.

While most anti-virus products will detect these messages as a malicious email, producers are urged to contact the NAIC Service Desk at (816) 783-8500 or help@naic.org if they receive a similar email or have any concerns.

To help you and your staff keep your personal information secure, we've compiled five, easy ways to avoid phishing attacks at work and at home:

1. Check the sender's email address. Phishing emails will masquerade as legitimate emails from IT, Microsoft or other well-known companies like the NAIC. For example, "FrankMuth@f-mins.com" looks very similar to "Frank.Muth@fmins.com."

2. Watch for unusual or alarming tones. Phishers may try to pressure you to respond quickly with suspicious messaging, such as "Your account will be deactivated!" or "Please review the attached document immediately."

3. Be skeptical of sharing requests. If you receive a suspicious email requesting sensitive information, use caution. Be sure you're only sharing sensitive documents and information with authorized parties.

4. Leave links alone. If an email link directs you to any login page – STOP. Phishers now target users for their work credentials rather than trying to compromise computers with malware.

5. Monitor staff, client and carrier emails. Be aware that even a staff member, customer or carrier employee's email account could be compromised. Instead, use other contact methods, such as by phone, to verify an unusual email is legitimate. And, always use a phone number on file instead of any phone numbers provided in the sender's email signature.

For more tips, feel free to see a complete list of cyber security blogs at fmins.com/blog. And, if you believe that you have fallen victim to identity theft, we can help. All Patriot Insurance agency partners, their staff and families have FREE 24/7 access to fraud specialists through our identity theft resolution partner, CyberScout, who can help determine the best course of action for you and your business or family.

For questions, please feel free to reach out to your field manager or underwriter.