ALLIED WORLD // FrameWRX℠

Nothing breeds more Cyber attacks like Success

Bad actors continue to threaten organizations by broadening their social engineering scams using more sophisticated methodology like **spoofed phone calls ('vishing') and texts ('SMiShing').** Vishing and SMishing attacks:

- Prey on organizations who cannot conduct in-person verification while telecommuting
- Make it easier to evade security tools
- Allow direct access to employees, making them the first line of defense

Allied World's Cyber insurance clients are now empowered with new tools to combat susceptibility to these attacks. Heightened awareness and training have proven key to mitigating social engineering. Our Allied World//FrameWRX℠ risk management platform offers insureds the ability to test their staff though simulations, using email, phone or text methodologies.

The platform, available via *Bait & Phish*, provides all the technology needed to provide a true simulated 'spoofing' experience, including the sense of urgency hackers use to trick unwitting victims.

At no additional cost, our Cyber insureds have access to:

- Two customized, managed social engineering campaigns per policy term
- Unlimited self-managed campaigns via a user-friendly interface
- Multi-method social engineering simulations (phishing, vishing and SMiShing)

After each campaign, insureds receive results to help them understand user behavior, create awareness, and close behavior gaps. Education/training videos based on user responses are available to boost employee vigilance, increase awareness, and avoid attack susceptibility in the future.

Contact AWFrameWRX@awac.com or your Allied World Cyber underwriter to learn more about our FrameWRX platform, including the social engineering services we offer.

ALLIED WORLD
A FAIRFAX Company