Everyone Is Working From Home Let's Go Phishing!

Working Remotely Makes It Harder To Spot Phishing Exploits

IMPACT:

- **Attackers are taking advantage of more remote workers and lax end-user training**
- **Less than one quarter of businesses under 500 employees have employed frequent end-user security training, education and applied testing regularly**
- **Whale Phishing more popular (targeting executives working from home ~ they know you)**
- **Impersonation fraud Phishing has jumped during the first 100 days of the pandemic**
- **Phishing success is almost guaranteed – is it work the risk to your business?**
- **Ethical Implications | Hackers don't care**

Be Aware: Impersonation Fraud Via Email Is On The Rise

Phishing attacks continue to pose problems for businesses around the world and, according to *The State of Email Security 2020* report from cybersecurity company Mimecast, 60% of organizations believe it's inevitable that they'll fall victim to an email-based attack over the course of the next year.

This could range from simple phishing, where an employee could be tricked into opening a malicious attachment or clicking on a bad link, to business email compromise (BEC), where attackers impersonate execs to eventually make off with large payments as a result of fraudulent financial transfers.

In an office, it is relatively simple to check if an executive had sent a request for a business bank transfer by walking over and asking if they'd sent the message – but with people suddenly working from home, making those checks isn't so simple.

Those classic impersonation requests are now more susceptible to attacks aggressively encouraging individuals to perform an action such as carrying out wire transfer or sharing sensitive data without verification. Executive beware; hackers know who you are and are experts at imitating you to your employees.

The fact that people working from home have become so inclined to communicating via email that they don't realize to check with colleagues via other channels. But despite the known threat posed by phishing and other email attacks, a high proportion of organizations – almost 60% – don't provide any sort of email security training on a frequent basis.

If something could be leaving your network, would you know before it is too late? Are your remote workers susceptible to cyberattacks? Organizations must ensure that people are properly informed about online risks.

Regular awareness training based on current threats is a must. By educating staff, from the board level down, make all employees security decision makers. Ensure that employees can spot suspicious activity when it occurs, what to do, understand the risk of the malicious activity and manage their company-issued devices.

Allow us to show you how we can make your remote workers Human Firewalls. Contact us at (954) 324-3478 or info@duolark.com.

Research by: Karl Norris | DUOLARK Founder & CEO
For more information please contact us (954) 324-3478 | info@duolark.com | www.duolark.com
June 9, 2020