Take These 3 Steps to Protect Your Data from Phishing Scams Targeting A Hybrid Workforce

Everyone is hustling a little harder these days. With the transition back into the office, and a hybrid workforce that is here to stay, bad actors are launching a new cyberattack every 39 seconds. They're hungry for data to sell in booming dark web markets — and no business is too small to fall victim to a phishing-related disaster like ransomware as two in five SMBs discovered in 2020.

Your hybrid workforce provides a target-rich environment for cybercriminals to exploit through phishing attacks. It only takes one employee opening a bogus email, clicking on a dangerous link or downloading a malware-laden attachment for your business to join the more than 75% of companies that were impacted by a phishing attack last year.

Here are three ways that you can act immediately to secure your remote workforce against phishing and prevent your business from becoming a cybercrime statistic.

1 Plan, Preserve, and Protect

It's critical to develop and practice an incident response plan to ensure that everyone can respond smoothly in case of an emergency. Experts recommend a layered approach to security to increase cyber resilience, including improving incident response times by adding security automation. Review your cybersecurity posture with an outside expert for an unbiased assessment and immediately address any gaps — with cybercrime up by more than 80% last year, there's no time to lose.

2 Trust but Verify

Even savvy staffers might still fall for a phishing attack, so make secure identity and access management (SIAM) a priority. Prevent mistakes from becoming disasters with multifactor authentication to take the power out of a stolen credential. Make it easy for security personnel to quickly respond to and contain incidents or mitigate phishing damage by using single sign-on. Plus, your IT team will be extra thankful if your SIAM solution also includes automated password resets eliminating a major source of needlessly time-consuming call tickets.

3 Make Prevention a Priority

The number one cause of a data breach never changes: human error. Ensure that everyone from the interns to the CEO are undergoing security awareness and phishing resistance training at least quarterly for training to stick. Make it easy and encouraged for staffers to reach out for help if they receive a suspicious message. Create a strong cybersecurity culture that makes everyone feel like they're an important part of the security team to transform your largest attack surface into your biggest defensive asset.

Don't wait to implement updates to your security posture that fight back against phishing-related cybercrime. Phishing risk is only growing larger — exploding by more than 600% in 2020. By ensuring that your staff is making smart choices about email handling, you can reduce the risk that your business gets hooked by a clever cybercriminal lure this year.