KnowBe4

Human error. Conquered.

Protecting Americans from COVID-19 Scams

Testimony before
Committee on Science, Transportation, Commerce

Subcommittee on Manufacturing, Trade, and Consumer Protection

United State Senate

July 21, 2020

2:30 p.m. EST

Mr. Stu Sjouwerman
Founder and Chief Executive Officer, KnowBe4, Inc.

Mr. Chairman and members of the committee, thank you for the opportunity to provide my perspective as Congress works towards developing solutions for businesses and governments combatting COVID-19 related scams and what more can be done to protect the public.

My name is Stu Sjouwerman, and I am the founder and Chief Executive Officer of KnowBe4, Inc., headquartered in Tampa Bay, FL with offices in Europe, South America, Australia and South East Asia.

KnowBe4 is the provider of the world's largest security awareness training and simulated phishing platform. Our services are used by more than 33,000 organizations around the globe. For the last 30 years, I have served as an entrepreneur and data security expert in the IT industry, and co-founded the Inc. 500 company Sunbelt Software, which was a multiple award-winning anti-malware software company that was acquired in 2010.

Realizing that the human element of security was being seriously neglected, I decided to help organizations manage the problem of cybercrime's social engineering tactics through new school security awareness training which is why I founded KnowBe4.

More than 33,000 organizations in a variety of industries -- including highly-regulated fields such as healthcare, finance, energy, government and insurance -- have mobilized their end users as their last line of cyber defense using KnowBe4.

KnowBe4 is founder-led and mission-driven. Our primary objective is to enable employees to make smarter security decisions by training them to become a "human firewall" in defense against social engineering attacks, which are responsible for upwards of 93% of data breaches.

The shutdowns and economic turmoil of the coronavirus pandemic have expanded the cyber attack surface, making it even easier for hackers and scammers. Ransomware and malware attacks are up, and users working from home are more susceptible to phishing attempts and other social engineering tactics to gain access to networks. If we don't focus on the human element - consumers and employees - we ignore a crucial part of cyber security.

Covid-19 has quickly reshaped the cyber threat landscape. For example, over 192,000 coronavirus-related phishing attacks have occurred per week over the last month. No one is immune to being scammed, and different types of scams target different sets of consumers. Scammers go to great lengths to make their attacks as convincing as possible, and many of these scams have very few visible signs that could tip off recipients. Consumers should not assume they can spot every scam attempt, and that bias only helps the scammers. The best way to fight scammers is educating consumers and employees with a combination of security awareness training *and* frequent social engineering testing.

New data from security vendor Tripwire highlights how the shift to remote working has changed the face of cybersecurity for both the current and future work climate. According to their report, 94% of organizations are more concerned about cybersecurity than before COVID-19 -- and they should be. The fact is, people are clicking on simulated COVID-19 phishing attacks at high rates and Coronavirus themed emails are rampant.

Malicious actors are aggressively exploiting the COVID-19 crisis by re-purposing and overhauling the phishing emails they were running before the Coronavirus emerged in late December. Although the bad guys have been developing new social engineering schemes uniquely based on the onslaught of recent events, these COVID-19 "re-treads" are fast becoming the most common variety of Coronavirus-themed phishing emails that we encounter on a day-to-day basis.

It’s no surprise that phishers and scammers are using the avalanche of new information and events involving the global coronavirus pandemic as a way to successfully phish more victims. These phishing scams are becoming more aggressive and more targeted as this pandemic continues. COVID-19 phishers prey on both consumers and employees and have sought private information through targeting passport details, the healthcare industry, social media channels, and we can expect to see them use current and future COVID-19 lawsuits as bait in spear phishing attacks. Everyone should remain very skeptical of any email related to COVID-19 coming into their inbox.

The emphasis in cybersecurity has traditionally been on hardware and software. However, we cannot solely rely on that. This strategy cannot catch everything, nor does it address the need for a human firewall. The largest breaches in our country - to include John Podesta’s personal email, our U.S. power grid, JP Morgan Chase, Sony Pictures, etc., - these systems relied on hardware and software for defense, yet still fell victim to phishing attacks.

Through new-school security awareness training, the likelihood of such social engineering attacks are significantly decreased, and organizations are inoculated against the types of compromises we’re seeing today.

Any support from Congress that would direct government agencies to implement ongoing security awareness training - more than the annual training typically in place - and include frequent social engineering testing would be greatly beneficial as we work together to bridge the gap in cyber security and protect American networks.

Thank you for the opportunity to share KnowBe4’s perspective on cybersecurity and our industry’s unique ability to protect American citizens from rising COVID-19 related social engineering scams. We are grateful to Chairman Moran and the members of the committee for the time and effort you all are putting into this important matter of national security. KnowBe4 is committed to being a helpful partner going forward as we all work to serve the best interest of the public.