How to Stop Employees from Falling for Cyber Bait

Cybercrimes have been on the rise over the past several years, and remote work has only made it more difficult to mitigate those risks. Nearly 50% of companies reported falling victim to fraud in the past 24 months, the second highest reported level in the last 20 years, according to a PricewaterhouseCoopers fraud survey . Businesses also reported roughly $42 billion in losses in the last two years due to fraud.

HP Inc.'s report, *HP Wolf Security Blurred Lines & Blindspots*, assesses organization cyber risk in an era of remote work. The report shows that changing work styles and behaviors are creating new vulnerabilities for companies, individuals and their data. According to the findings, 70% of the office workers surveyed admitted to using their work devices for personal tasks, while 69% have used personal laptops or printers for work activities. Almost one-third (30%) of remote workers surveyed also have let someone else use their work device.

As a result of these and other behaviors, employees working from home are increasingly being targeted by hackers.

48% of company board directors are concerned about cybersecurity, according to a Gartner report, *3 Steps to Stop Employees from Taking Cyber Bait*. So, it is more crucial now than ever to prepare employees so they can help protect the company.

"Cybercriminals have become experts at social engineering skills, tricking employees into clicking on malicious links that initiate attacks. While security and risk management leaders know that social engineering is a top risk, many still struggle to stop employees from taking the bait," according to the report.

The first step is raising employee awareness. Try developing a list of *signature behaviors* for employees, like reporting suspicious emails to security, using passphrases to create strong passwords and using secure file transfer solutions.

Make sure employees keep an eye out for unusual phrasing and poor grammar in an email. That's usually the first red flag of potential fraud. Double check to make sure the email address is legitimate and from an official source.

Another way to help boost cybersecurity awareness is by measuring behavior outcomes instead of actual activities. For example, instead of measuring the number of phishing simulations, the report recommends measuring phishing simulation click rates. Instead of looking at the number of training modules created, try looking at the average phish report rates. And measure the percent decrease in data loss prevention alerts instead of the number of newsletters published.

Connecting awareness about cybercrime to business benefits is also crucial in getting the entire company on board, the report says. Layout the map from initial employee education about phishing and ransomware, which leads to changed employee behavior, and ultimately equates to reduced cost and increased productivity.

"If you ever have any doubts about the legitimacy of an email, you should forward it to your IT department to be safe," said Robert Karau with Merchant & Gould P.C. (Minneapolis, MN). "Use commonsense and think things through before responding to certain requests,"