# US workforce 'unprepared' for cybersecurity threats - new study

FORT WORTH, TX, UNITED STATES, September 25, 2025 /EINPresswire.com/ -- A new report has revealed that over one quarter (26%) of employees in the US have never received cybersecurity training from their employer, including receiving guidance on hacking attempts and phishing scams.

The new report from RS, a global provider of product and service solutions for industrial customers, surveyed 1,000 US-employed individuals across the nation.

The study saw RS survey 1,000 workers from different industries, and found that many workers are committing basic cybersecurity errors.

The research found employees commonly committed the following:

Used the same password for multiple platforms (46%)
Stored passwords on a work laptop, phone, or writing pad (31%)
Left desk without locking/logging out of/shutting down computer (28%)
Chosen to avoid using two-factor authentication for logins (26%)
Failed to update software on time (25%)
Used a password with name or birthday in it (24%)
Worked from an unprotected Wi-Fi source (e.g. open Wi-Fi that is not password protected) (20%)

Clicked on a link from an unverified source (20%)
Opened a document from an unverified source (18%)
Sent confidential data or files to the wrong recipient (9%)

A third of Americans (32%) who were surveyed described themselves as either neutral or ‘unprepared’ for any cybersecurity threats.

The data also found that almost one third (72%) of employees are likely to use their personal devices for work purposes – this is particularly true for those aged 16-24, who are much more likely (78%) to use their personal devices for work, compared to 55+ year olds (60%).

The cybersecurity threat continues even when working from home, as over half (62%) Americans don’t use a firewall when working from home and less than a third (32%) join a work VPN.

Jared Parker, Security Compliance Manager at RS, commented: “Surveys of this nature play a vital role in evaluating the effectiveness of cybersecurity training programs currently implemented across organizations.

“As work from home and Bring Your Own Device (BYOD) policies become increasingly prevalent, the threat landscape continues to evolve, making it imperative for companies to equip employees with up-to-date knowledge on emerging security threats and tactics employed by malicious actors.

“Cybersecurity education can no longer be treated as a one-time annual compliance exercise, as critical information is easily forgotten without regular reinforcement. Instead, organizations should adopt a continuous learning approach by delivering concise, easily digestible training nuggets throughout the year.

“These micro-learning modules should focus on helping employees recognize and respond to the latest emerging threats, especially as adversaries leverage advancing technologies like artificial intelligence to refine their attack methods and techniques.”

Rhys Thomas
IDHL
+44 845 340 3799
email us here