

# Cyber Security Awareness Month: it's not another Hallmark Holiday

*With sophisticated cybersecurity incidents on the rise, companies are using October Cybersecurity Awareness Month to engage their weakest link: employees.*

ATLANTA, GA, USA, September 28, 2022 /EINPresswire.com/ -- The numbers tell all: breaches are rising, and hackers are targeting our employees. Cybercrime victims in recent weeks include Uber, SeeSaw, Holiday Inn, and Rockstar Games.

Breaches due to employee mistakes are on the rise. "People are one of the biggest risks to enterprise cybersecurity," says [Doug Saylor](#), a

partner, and co-leader of ISG Cybersecurity. "Some 85% of breaches today involve human error, with breaches caused by phishing attempts up 25% in the last year.



Thousands of organizations use Employee Cybersecurity Awareness Month to reduce cyber risk

“

The key to employee engagement in cybersecurity is delivering content they want to read, not that they must read to check a box.”

*Aware Force CEO Richard Warner*

According to Verizon's 2022 Data Breaches Investigations Report, the number sits at 82% of data breaches involving a human element.

Most companies have cyber security training programs in place. That's good. But most programs usually involve once-a-year or quarterly testing, occasional surprise quizzes, and white papers they hope will get read. So, if I.T. teams are doing this, why are cyber issues on the rise?

The answer is twofold. First, the bad guys are getting savvier and more aggressive. And second, the good guys on the receiving end maintain the status quo. Remote work adds to the problem. So, to better protect our organizations, we must do a better job of engaging our employees.

Enter Cyber Security Awareness Month. It's the one month a year when all eyes are on I.T. Security. This is our opportunity to grab employees' attention. But come November, most employees will have forgotten what they learned in October.

There's scientific proof of that. Ebbinghaus's Forgetting Curve, the influential memory model, shows that the information we learn rapidly slips from our memory over time unless we work to keep it there. By some estimates, 75% of cybersecurity training is forgotten by the end of the day...90% by the end of the week.

So, why stop engaging employees at the end of October? Why not provide engaging cybersecurity content to employees consistently, year-round?

Most would say that good content is hard to find. And will employees take time to read what we put out?

Richard Warner, CEO of Aware Force, says, "the key to employee cybersecurity engagement is delivering content they want to read, not that they must read to check a box."

"The Aware Force team learned early on that cybersecurity content must be snackable (easy to read and understand), topical (covers current events that employees can do something about), and interactive (a mix of videos, quizzes, and clickable exercises that are fun). That's what we deliver year-round. All of it branded for the client."

The Aware Force model is delivering interesting cybersecurity content to employees year-round, branded and tailored for each customer, using a process that is cost-effective and easy to distribute. Aware Force has a 95% renewal rate and dozens of unsolicited comments from employees praising the content — often saying they share it with family members.

For October Cybersecurity Month, Aware Force doubles its production schedule and delivers Cybersecurity Posters with each client's branding. Click to view a sample of the Aware Force employee cybersecurity newsletter for [October Cybersecurity Awareness Month](#). (This example uses Aware Force branding.) Aware Force cybersecurity content is available in English and



The graphic features the Aware Force logo at the top, followed by the text "Cybersecurity news from the Aware Force Cybersecurity Team". Below this is a background image of a computer keyboard with the text "Protect Your Digital Identity" and "Here's what four big cyber breaches of the past few weeks have taught us." At the bottom of the graphic is the Aware Force logo again, with the text "Aware Force cybersecurity news lead for October 1 edition: Lessons from recent cyber hacks" above it.

**Aware Force**<sup>®</sup>

Cybersecurity news from the  
Aware Force Cybersecurity Team

**Protect Your Digital Identity**

Here's what four big cyber breaches  
of the past few weeks have taught us.

Aware Force cybersecurity news lead for October 1  
edition: Lessons from recent cyber hacks

**Aware Force**<sup>®</sup>

Canadian-French versions.

Suzanne Cassada

Aware Force

+1 470-448-3887

cutrisk@awareforce.com

Visit us on social media:

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/593228054>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.