aci LEARNING | AUDIT. CYBER. IT.

CYBERSECURITY AWARENESS

Protect Your Business.

Why cybersecurity awareness training is a must.

Overview

In the modern digital age, our personal and professional lives are lived – and stored – increasingly online. While there is much to be enjoyed about the ease of having the world at our fingertips, it is also easier than ever for hackers to find and access targets. Cybersecurity and data breaches happen every day, and the cost that companies now face – and consumers often pay – is forcing businesses to recognize that cyber awareness training is critical to future-proofing operations. Last year, over 422 million individuals were affected by company data compromises.

With our daily lives taking place increasingly online, no one is immune to cybersecurity threats, but some industries are at greater risk of private data violations due to the type and volume of personal information they store.

> In 2022, healthcare, financial services, and manufacturing were the three industry sectors that recorded the most data breaches.

Employee cybersecurity training is no longer optional but a must in order to work productively without exposing both the company and the individual to safety issues.

TABLE OF CONTENTS

WHAT TO EXPECT

In this e-book, you will learn what cybersecurity awareness training is, examples of some of the most infamous data breeches of our time, how training employees protects them, your company and your customers and why your company cannot afford to skip it.

BY THE NUMBERS

Worldwide large data exposures

2013

3 BILLION RECORDS

Yahoo experienced one of the largest ever data breaches, dating back to 2013. The company first reported about 1 billion exposed records, then later came up with an updated number of leaked records, which was 3 billion.

2018

1.1 BILLION RECORDS

India's national identification database Aadhaar was breached with over 1.1 billion records exposed.

2020

11 BILLION RECORDS

An adult streaming website, CAM4, experienced a leakage of nearly 11 billion records.

2022

25.6 MILLION RECORDS

LastPass password-manager experienced a breach, leaving 25.6 million users' password vaults and other personal information vulnerable. A second incident later occured and allowed attackers to go through the company's cloud storage and sensitive data.

PROTECT YOUR ASSETS

Why companies cannot afford to skip cybersecurity awareness training

In 2022, the averaged cost per data breach was $4.24 million and 38 percent of companies lost business because of a breach, which accounted for over half of the total financial losses.

> 95 percent of breaches are caused by human error. No amount of technical prevention or firewalls can keep a staff member from falling for a phishing email.
>
> ***Source:*** *The IBM Cybersecurity Intelligence Index*

It's clear that employees are the frontline of a company's security measures, and therefore they must be appropriately prepared on the best way to spot and react to cyber-attacks.

To avoid security breaches, loss of productivity and reputational damage, companies must have a cybersecurity awareness program.

WORKFORCE TRAINING

What is cybersecurity awareness training?

Cybersecurity training helps employees learn how to identify potential threats and respond appropriately. It also provides employees with the knowledge and skills needed to recognize, report, and prevent cybersecurity incidents.

Creating and implementing such a sweeping program throughout an organization can seem like a daunting task for any business, but the reality is that the cost of not training employees is too high to ignore.

By training your workforce to recognize these attacks, you can significantly reduce the risk of a security incident or breach. It might sound simple, but how many of your employees can identify the signs of a phishing scam and know that they should not open the email but instead forward it to IT professionals in the company for vetting?

We know cyber training.

ACI Learning can help implement cybersecurity awareness training

Our new CyberSkills program is designed to empower your workforce to stay safe, protect your company's data and recognize signs of a cyber-attack.

SOCIAL ENGINEERING

Help prevent sensitive information from falling into the wrong hands and protect against a variety of threats, including phishing attacks, pretexting, baiting, and quid pro quo. By teaching employees how to identify and respond to these tactics, organizations can significantly reduce the risk of falling victim to social engineering attacks.

PASSWORD SECURITY

Having a secure password can help protect your personal and sensitive information from being accessed by unauthorized individuals. A strong password is difficult for others to guess or crack, making it more difficult for cybercriminals to gain access to your accounts or devices. Using unique, complex passwords for each of your accounts can also help prevent one compromised password from being used to access multiple accounts. Overall, using secure passwords is an important aspect of protecting yourself and your information online.

NETWORK SAFETY

Having safe networks can help prevent unauthorized access to the organization’s devices and data and can also help protect against cyber-attacks and data breaches. Using secure protocols and encryption can help to ensure the confidentiality and integrity of data transmitted over the network. Additionally, implementing network segmentation and using firewalls can help to further protect the network by limiting access and controlling the flow of traffic. Overall, having safe networks is an important aspect of protecting an organization’s cybersecurity.

MALICIOUS SOFTWARE

Malicious software, or malware, is any software that is designed to harm or exploit vulnerabilities in computer systems. By teaching employees about the types of malware, how it spreads, and how to identify and avoid it, an organization can help prevent malware infections and the potential damage they can cause. This can include things like phishing attacks, ransomware, and other types of malware. Overall, having a high level of malware awareness can help to strengthen an organization’s defenses against cyber threats.

PHYSICAL SECURITY

Having physical security measures in place can help an organization protect against cyber threats by creating an additional layer of defense. These measures can include secure access controls, such as keycards or biometric scanners, for physical locations; secure storage for devices and data; and surveillance cameras to help detect and deter unauthorized access.

By implementing physical security measures, an organization can help prevent unauthorized access to its devices, data, and physical locations, which can in turn help protect against cyber attacks and data breaches.

BE BOLD. TRAIN SMART.

Looking for more binge-worthy cybersecurity training from ACI Learning?

Cybersecurity Workplace Training teaches learners how to protect organization data and systems from cyber threats, recognize various threats and vulnerabilities and best practices with respect to cybersecurity and incident response.

Finally, this course will touch on regulatory compliance and ways in which audits of cybersecurity workplace training can influence and strengthen awareness programs.

Explore course catalog

Sources:

7 reasons why security awareness training is important in 2023
www.cybsafe.com

6 Reasons Why Your Employees Need Cybersecurity Awareness Training | Aware | EC-Council
www.eccouncil.org

Cybersecurity Awareness: What It Is And How To Start
www.forbes.com/advisor

[AUDIT] [CYBER] [IT]

Start your training!

Technology (and vulnerabilities) are constantly changing. Your training should to. That's what we do best. Contact us today to learn more.

Train smart

(866) 378-0761
www.acilearning.com
hello@acilearning.com

ACI Learning is a leading certification prep and skills training provider of audit, cybersecurity and IT training solutions designed for individuals and enterprises.

We take training to the next level with our SaaS platform that supports multiple learning styles – instructor-led, online video self-paced, hands-on and real-life labs and assessments – and provides insight.

aci LEARNING

Be bold.
Train smart.