Cybersecurity Starts With Training Your Team

Stay ahead of social engineering attacks with expert awareness training and testing, one of our Big Security solutions to help keep your data safe.

As malicious cyber threats increase and evolve, so should your employee awareness. After all, your employees can't protect your business if they don't know what threats look like.

Whether your team needs the fundamentals or a readiness refresher, an interactive computer-based simulation program from Barracuda® can help your team get the cybersecurity training they need to protect your business.

COMMON RISKS EMPLOYEES FACE AND WHAT YOU CAN DO ABOUT IT

PHISHING ATTACKS

Deceptive emails and messages trick employees into sharing sensitive information or clicking malicious links that give hackers access to your sensitive data.

WHAT YOU CAN DO

Provide simulation training, so your team can quickly spot phishing attempts and suspicious emails.

WEAK PASSWORDS

Hackers exploit users daily with easy-to-guess or recycled passwords that give them access to your sensitive data and systems.

WHAT YOU CAN DO

Offer awareness training to teach your team the aspects and benefits of strong, unique passwords.

IMPROPER DATA HANDLING

Sharing unencrypted data or leaving it unsecured opens your company to serious risk.

WHAT YOU CAN DO

Training helps your employees understand how to safely handle sensitive data and follow security protocols.

LACK OF SECURITY AWARENESS

If your employees don't recognize a threat or attack, they can't prevent it or alert your security team to respond quickly.

WHAT YOU CAN DO

Tap our expert training and testing solutions, including a premium concierge service, to help your team exercise a security-conscious mindset, so they spot red flags and see threats coming.

WHAT'S AT STAKE?

If a breach occurs, it's not just about financial and reputational loss. Your business itself is on the line, as sixty percent of small businesses close within six months of a cyberattack.[1]

68%
of data breaches stem from human error.[2]

$9.5M
average cost of a data breach in the U.S.[3]

2 OUT OF 3
breaches are **NOT** identified by an organization's own security teams or tools.[4]

SO WHERE SHOULD YOU START?

Train your team how to be your first and best line of security defense. Our expert consultants can:

- // Develop a customized training approach based on your organization's unique needs.
- // Test your team's security awareness through an interactive simulated phishing platform.
- // Collect and review detailed metrics.
- // Conduct security training based on recommendations.

INTRODUCING CONCIERGE

Need us to handle it all? Let us do the heavy lifting through a premium concierge service. Our experts will define the scope of your phishing simulation campaign and then configure, execute, analyze the findings, and offer recommendations tailored to your business.

Find out through expert campaigns that test your team's response to phishing and other cyber threats so you know where you stand and can implement new protocols.

BEFORE SECURITY AWARENESS TRAINING

- An urgent email from the CEO? Better open it fast.
- Well, "p-a-s-s-w-o-r-d" is easy to remember, so I'll use that.
- I'll only be gone from my computer for a minute.
- Cybersecurity is IT's job, not mine.

AFTER SECURITY AWARENESS TRAINING

- An urgent email from the CEO? Typical phishing attempt, better report it.
- So long, "p-a-s-s-w-o-r-d"! I know how to create super strong passwords now.
- Data is important. I'll handle both digital and physical information with the care it deserves.
- Wow, I have more power and responsibility than I thought. I keep security top of mind while using company systems for work or personal use, especially social engineering attempts. I don't want to be the reason data is compromised.

SECURITY IS AN ONGOING TEAM EFFORT

Give your team the tools and training to keep your organization running smoothly and safely. Because business as usual is the best outcome.

Canon U.S.A. can help connect you with top-notch security education and training so your team learns what to watch for—so they can be your best defense. That's why Big Security is truly for everyone at your organization.

THE 5 PILLARS OF SECURITY

DEVICE SECURITY
DOCUMENT SECURITY
MOBILE SECURITY
CYBERSECURITY
INFORMATION SECURITY

Canon U.S.A.'s Five Pillars of Security presents a portfolio of cybersecurity products and services in a comprehensive way that groups solutions in functional areas. Cybersecurity is a key component of our Five Pillar approach.

For more information about cybersecurity and Canon U.S.A. 5 Pillars of Security contact us today or visit our website at USA.CANON.COM/SECURITY.

[1] U.S. National Cyber Security Alliance, 2023.
[2] Verizon, 2024 Data Breach Investigations Report, 2024
[3] IBM Cost of a Data Breach Report, 2023.
[4] IBM Cost of a Data Breach Report, 2023.

Many variables can impact the security of a customer's device and data. Canon does not warrant that the use of services, equipment, or related features will eliminate the risk of potential malicious attacks, or misuse of devices or data or other security issues.

11/25-0139-9369