



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Vijayan, Jai

Title: “7 Tips for an Effective Employee Security Awareness Program”

Website: Dark Reading Threat Intelligence

Organization: Dark Reading

Date: 17 April 2019

URL: https://www.darkreading.com/threat-intelligence/7-tips-for-an-effective-employee-security-awareness-program/d/d-id/1334416?image_number=8

Accessed: 12 July 2019

Synopsis: Employee security awareness training programs have become a necessity for organizations in recent years because of the high percentage of data breaches caused by careless and negligent workers.

Phishing, in particular, continues to be a top attack vector because of the success threat actors have in tricking employees into downloading malware on their systems or following links to malicious sites. Many data breaches are also the result of poor employee password security habits and the failure to follow enterprise policies for data access, use, sharing, and storage.

In fact, negligent employees are one of the highest security risks for organizations in the US and elsewhere, according to a 2018 study by Shred-It. Eighty-four percent of C-suites and 51% of small-business owners described such employees as their biggest security problem. Ninety-six percent of Americans hold negligent employees as least partly to blame for data breaches at major US companies.

"While data breaches that grab headlines are often perpetrated by external threats, at least half of all security breaches are carried out by insiders," says Chris Olson, CEO of The Media Trust. This can include malicious insiders, negligent employees, and third parties with access to the enterprise network.

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan Slideshows

Breaches and compliance requirements have heightened the need for continuous and effective employee training, security experts say.



1 of 8



Image Source: Shutterstock

Employee security awareness training programs have become a necessity for organizations in recent years because of the high percentage of data breaches caused by careless and negligent workers.

Phishing, in particular, continues to be a top attack vector because of the success threat actors have in tricking employees into downloading malware on their systems or following links to malicious sites. Many data breaches are also the result of poor employee password security habits and the failure to follow enterprise policies for data access, use, sharing, and storage.

In fact, negligent employees are one of the highest security risks for organizations in the US and elsewhere, according to a 2018 study by [Shred-It](#). Eighty-four percent of C-suites and 51% of small-business owners described such employees as their biggest

security problem. Ninety-six percent of Americans hold negligent employees as least partly to blame for data breaches at major US companies.

"While data breaches that grab headlines are often perpetrated by external threats, at least half of all security breaches are carried out by insiders," says Chris Olson, CEO of The Media Trust. This can include malicious insiders, negligent employees, and third parties with access to the enterprise network.

But breaches are not the only reason for employee training. Many regulations, including PCI and HIPAA, mandate regular employee security awareness training. While requirements for such training can vary, the goal is to ensure companies take measures to address risks posed by employees and other insiders with trusted access to enterprise networks and assets.

Here, experts share some of the key attributes that make up an effective employee security awareness training program.

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... [View Full Bio](#)



1 of 8



More Insights

Comments



Rate It



50%



50%

[REISEN1955](#),

User Rank: Ninja

4/17/2019 | 10:36:38 AM

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan *Slideshows*

Assess and Identify the Problem Areas

Before you get started, do an initial assessment to identify the problem areas, says Amy Baker, vice president of security awareness training strategy and development at Proofpoint. The assessment can be anything from a broad phishing test to a question-based cybersecurity knowledge assessment. "This knowledge can be used to inform the larger program that the organization rolls out, as each module selected can be targeted to improve a specific problem area identified in the assessment," Baker says.

But don't just assess current security capabilities and knowledge. Also evaluate employee attitudes before rolling out a training program, advises Lisa Plaggemier, chief evangelist at Infosec, a provider of IT security education and workforce security awareness services. "Do they view security as a roadblock, a barrier to time to revenue, or the 'department of no?'" she says. "If so, you've got to change the culture, not just train people to spot phishing emails."

In addition, remember that you can't have a one-size-fits-all security-training program. Different roles have different needs, so you need to approach your program that way, too, Plaggemier says.

Image Source: Shutterstock

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan *Slideshows*

Focus on the Phishing

Employees who click on phishing emails are one of the most common reasons for data breaches these days. Teaching employees how to recognize and avoid such emails is fundamental to security, experts say. "While social engineering, in general, must be addressed, phishing should be the primary example and focus," says Anurag Kahol, CTO and co-founder of Bitglass.

Phishing attacks use impersonation and other deceitful tactics to trick users into surrendering their credentials or access to their accounts in other ways. So it's vital to emphasize the need for strong passwords and highlight the dangers of password reuse, especially across personal and corporate accounts, he says.

Even security-conscious organizations continue to be targeted by phishing attacks. "Consequently, employees must be shown how to identify the signs of phishing, such as strange email domains, typos, unusual communications, and more," Kahol notes.

Also important is the need to inform employees about how and why they could become targets based on their individual roles in the organization, says Vinay Pitahaya, director of security research at Menlo Security.

When training employees, provide examples of a phishing attack or a simulated attack that is representative of their day jobs to make them aware of the impact of their actions and how easy it is to be the first victim, he adds.

Image Source: Shutterstock

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan *Slideshows*

Make the Content Engaging

If you don't want employees to tune out, make the training content engaging, says Oliver Münchow, security evangelist and founder of Lucy Security. "Keep the user engaged with a good mix of video, gamification, and tests," he says. Provide instant feedback and gratification via a diploma upon completion, for example, he says.

Also, develop group-specific content. "For example, an IT administrator does not need an explanation on how to clear a browser cache or what the domain part of a URL is," he says. "Customize the courses to align with company policies and regulations."

Every training program should contain content around building and protecting strong passwords, protecting sensitive organizational data throughout its life cycle, physical security of data and devices, staying safe on mobile devices, and recognizing insider threats, Proofpoint's Baker adds.

Image Source: Shutterstock

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan *Slideshows*

This site is operated by a business or businesses owned by Informa PLC and all copyright resides with them. Informa PLC's registered office is 5 Howick Place, London SW1P 1WG. Registered in England and Wales. Number 8860726.

Breaches and compliance requirements have heightened the need for continuous and effective employee training, security experts say.



5 of 8



Highlight the Scale at Which Attackers Operate

One way to get employees to think twice about their actions is to give them an idea of the scale at which attackers operate, says Brian Johnson, CEO and co-founder of DivvyCloud. Use scanning activity data, for example, to highlight how attackers are constantly trying to break into your environment. "Understanding the number of attackers looking to penetrate the organization on a daily basis by looking for common misconfigurations" can have a big impact, Johnson says.

Image Source: Shutterstock



7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan Slideshows

This site is operated by a business or businesses owned by Informa PLC and all copyright resides with them. Informa PLC's registered office is 5 Howick Place, London SW1P 1WG. Registered in England and Wales. Number 8860726.

Breaches and compliance requirements have heightened the need for continuous and effective employee training, security experts say.



6 of 8



Don't Just Focus on Work-Related Risks

Your employees have to deal with security risks both at work and at home. So make sure your training includes tips to help the stay secure in both locations, says Marie White, president and CEO of Security Mentor. "When employees understand that you are concerned about them, they are much more open to the messages that you are trying to teach," she says.

Helping employees stay secure on their personal devices also protects the enterprise because employees often bring and use the same devices at work, she says.

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan Slideshows

This site is operated by a business or businesses owned by Informa PLC and all copyright resides with them. Informa PLC's registered office is 5 Howick Place, London SW1P 1WG. Registered in England and Wales. Number 8860726.

Breaches and compliance requirements have heightened the need for continuous and effective employee training, security experts say.



7 of 8



Make Sure Your Program Is Compliant With Regulations

Many regulations, including PCI DSS, HIPPA, and several federal and state regulations, require companies to implement security-training programs. Make sure your program is compliant with the requirements for training programs contained in these regulations, Bitglass' Kahol says.

Make employees aware of these compliance requirements, The Media Trust's Olson adds. "The bottom line is that security and privacy are key to future-proofing your business," he says. "Forewarning employees means forearming them and the company."

7 Tips for an Effective Employee Security Awareness Program

Jai Vijayan *Slideshows*

Reinforce, Reinforce, Reinforce

If the goal is to change user behavior, a one-time or once-a-year training effort won't cut it. "We recommend regularly reinforcing training throughout the year using different tools and methods," Baker says. In addition to monthly or quarterly training sessions, some companies use posters, newsletters, and videos to remind employees about cybersecurity, she notes.

You need to keep at it even after significant improvements have been achieved, adds Shlomi Gian, CEO of CybeReady. A good training program is continuous, timely, adaptable, and localized in terms of the language and cultural context of the employee's location, he says. "Research shows that a monthly training session is the bare minimum to keep awareness top-of-mind without overwhelming employees," Gian adds.

Image Source: Shutterstock