WEBROOT
Smarter Cybersecurity™

Why Security Awareness Training is an Essential Part of Your Security Strategy

Best Practices for MSPs

Background

Every year, millions of people fall victim to cybercrime. Hackers and criminals prey on their victims using a wide variety of elaborate techniques such as phishing emails, ransomware attacks, and phony web pages, among others. In fact, scams that have plagued society for centuries only continue to grow in size, sophistication, and complexity. For instance, the well-known Nigerian email hoax has roots from a common "Spanish Prisoner" scam that dates back more than 100 years.[1] In this type of primitive "advanced fee scam," the fraudster requests cash in return for a large commission which, of course, is never delivered.

"Phishing attacks were responsible for 90% of successful network breaches."[2]

Today, cyber scams know no bounds. In no other time in history has it been so easy to target anyone, anywhere, anytime. Cybercriminals don't discriminate; consumers and businesses in all industries, large and small, are potential targets. As a matter of fact, small businesses are often targeted simply because they lack in-house IT security resources. What's more, due to the volume, velocity, and variance of today's threats, technology solutions cannot mitigate every potential breach.

How do we fall victim so easily? Most people want to trust and assist others in need. But today, this trusting nature is chronically exploited by cybercriminals looking to take advantage. We are constantly being socially engineered by those who want to harm, undermine, and steal from us. What's more, these cyberattacks are progressively more personal, making them barely detectable by even the most tech-savvy internet users.

"Last year, the FBI's Internet Crime Complaint Center (IC3) received a total of 298,728 complaints with reported losses in excess of $1.3 billion."[3]

Common Tactics of Cybercriminals

Being a good "cyber citizen" starts with a solid security education, and a certain degree of paranoia is necessary to protect users from modern cyber threats. In fact, nearly every form of digital communication has the potential to be compromised for someone else's gain.

This means it's important for everyone to educate themselves on the tactics criminals use. This responsibility places organizations and end users firmly in the driver's seat when it comes to protecting personal data, preventing identity theft, and maintaining business continuity.

» **Phishing and Spear Phishing**

Phishing is the use of unsolicited communication, such as email, SMS, or phone calls from a fraudulent company to obtain banking information, passwords, Social Security numbers, or other personal information. It can happen to anyone, and may be launched at a high number of recipients, expecting only a small percentage of return. Spear phishing has the same goals, but typically involves a specific target, and may require more research and interaction to gain that target's trust.

Most breaches occur when a victim responds to a phishing email or clicks a link in one and completes a form on a fake website or unknowingly downloads malware. For instance, Anthem, the parent company of Blue Cross and Blue Shield, encountered one of the largest breaches in history when five unsuspecting employees unwittingly downloaded Trojans and keyloggers from a phishing email. In this breach, up to 80 million medical records were stolen, resulting in more than $115 million dollars in settlement costs.

» **Whaling**

Whaling, like spear phishing, is a targeted form of attack. In this case, it aims to acquire sensitive information, funds, or other data from high-profile employees, c-level executives, and upper-level management. In this scam, the victim receives an email that appears legitimate, requesting wire transfers or information about sensitive data like tax information. In many cases, the hackers register domain names that resemble the victim's company or an entity like the Internal Revenue Service, which can easily be overlooked when the whaling email is received. Moreover, the emails and sites that serve up the scam appear remarkably authentic. With whaling, the stakes are high, and some managed service providers (MSPs) report that whalers have convinced executives to transfer funds exceeding $10,000.

» **Malware and Scareware**

Malware and scareware are distributed by cybercriminals to harm computers, steal personal data, solicit payments, and infect systems. There are a variety of techniques, but with these scams, end users may receive a warning from an illegitimate antivirus software company indicating they located infected files on the victim's computer. Next, they prompt the victim to purchase an antivirus application to remedy the problem. Unfortunately, the alleged fix is malware designed to steal the user's credit card data and other personal information, as well as to solicit payment.

» **Ransomware**

Due to its debilitating nature, ransomware is one of the most disruptive and prolific security threats in the modern security landscape. These attacks are designed to lock organizations and end users out of their computers, personal data, and networks to halt the availability of critical computer systems and files. In some cases, the goal is to collect a ransom. In others, hostile governments seek to disable businesses, financial institutions, airports, public utilities, and other entities. What's particularly dangerous about ransomware is its worm-like capabilities, which allow these attacks to quickly spread across computers sharing a network. Because of this, Ransomware can easily hold medical systems hostage and disable infrastructure, such as public transportation, power plants, and more.

[1] Charles Seif. "Virtual Unreality: Just Because the Internet Told You, How Do You Know It's True?" (June 2014)
[2] Verizon. "2017 Data Breach Investigations Report." (April 2017)
[3] FBI. "2016 Internet Crime Report." (June 2017)

"Last year, the FBI's Internet Crime Complaint Center (IC3) received 2,673 complaints in the United States identified as ransomware with losses of over $2.4 million."[3]

To date, two of the most prolific ransomware attacks are WannaCry and Petya, which both target computers running Microsoft Windows and extort victims by demanding a ransom in the Bitcoin Cryptocurrency to recover their systems. WannaCry alone has been reported to have infiltrated more than 300,000 systems in more than 150 countries. What's more, similar and more sophisticated attacks are circulating, such as NotPetya, which disabled organizations across Ukraine in 2017, causing hundreds of millions of dollars in damage.

In most attacks, cybercriminals get their foot in the door using social engineering tactics, such as phishing emails or Remote Desktop Protocol (RDP), which allows them to remotely connect to their victims' computers. Although keeping your computers' operating systems patched and up-to-date can help prevent a variety of attacks, there is nothing as effective as security awareness training to defend against ransomware and phishing.

» **Unsecured WiFi Hot Spots**

As the mobile workforce continues to flourish, end users frequently take advantage of WiFi hot spots. Many employees don't understand that using public WiFi can put them and their businesses in harm's way. Interception of communications via man-in-the-middle (MITM) attacks, packet sniffing, session hijacking, and spoofed access points are just a few of the techniques hackers utilize to steal data. Once an end user is connected to an unsecured access point, attackers can easily descend into their device with malware and other malicious actions. Security awareness training can help to combat these vulnerabilities by educating end users about the dangers of public WiFi, and best practices when using it.

» **Malicious Apps**

The Pew Research Center reports that roughly three-quarters of Americans (77%) now own a smartphone, which represents a major increase over the past 10 years.[4] Naturally, as more people adopt smart devices, attackers will increasingly target those users. According to the Webroot 2017 Threat Report, in 2016 nearly 50% of the new and updated mobile apps analyzed were classified as malicious or suspicious.[5] That means nearly 10 million dubious mobile apps were distributed that year.

Plus, as the "bring-your-own-device" movement continues to gain momentum, mobile apps can present a major challenge to security. They expose leakage and can even gain unauthorized access to data through malicious WiFi networks and other methods. Mobile device management mitigates some risks, but the evaporation of the security perimeter reinforces the importance of proper online hygiene, which is taught in security awareness training.

The Role of Security Awareness Training

With today's increasingly personalized and prolific cyberattacks, growing regulatory demands, and security skills shortage, emphasis placed on cybersecurity education goes a long way towards getting ahead of threats. But, the fact is, many organizations focus their security budgets on technology solutions, while underestimating the power of the "human firewall." Time and again, organizations that successfully keep threats at bay are utilizing a more holistic approach to IT security by balancing security awareness training and security technologies.

"There's a group of people who will click and open every single email in the world. And you know, in this day and age there's a few landmines out there, and they can cripple a company."

Jeremy Koellish, COO at TekTegrity, Inc.

Security awareness training educates users on security threats and best practices, and ensures they understand and follow the behavioral requirements. What's more, this is not a one-time practice; it engenders good cyber citizenship within an organization's culture, and reinforces to employees that they're the first line of defense against cyberattacks.

Plus, as the line between work and home continues to blur, employees should practice good online hygiene all day, every day. Employees often do not follow safe practices at home, which results in breaches at the workplace. Equally concerning, when they are at work, they may feel a false sense of security and let their guard down. Security awareness training is the perfect solution to combat these challenges.

Compliance Requirements

Security awareness training is not just a great way to protect organizations and give them peace of mind. In many industries and countries, it's the law. Financial services, healthcare, energy, and other sectors require end-user awareness training at the very least on an annual basis. Depending on the industry, organizations may face stiff fines for neglecting compliance training. And with the new General Data Protection Regulation (GDPR) regulations, security awareness training is essential for data protection compliance.

The list below includes, but is not limited to, regulations and policies that require security awareness training:

» 201 CMR 17.00: Massachusetts's Data Security Law

» FDIC: Federal Deposit Insurance Corporation

» FFIEC: Federal Financial Institutions Examination Council

» FISMA: Federal Information Security Modernization Act of 2014

» GDPR (May 2018): EU General Data Protection Regulation

» GLBA Safeguards Rule: Gramm-Leach-Bliley Act

» HIPAA: Health Insurance Portability and Accountability Act of 1966

[4] Pew Research Center. "Record shares of Americans now own smartphones, have home broadband." (Jan 2017)
[5] Webroot. "2017 Webroot Threat Report." (Feb 2017)

» ISO/IEC 27001 and 27002: Code of Practice for Information Security Controls

» NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

» PCI-DSS: Payment Card Industry Data Security Standard

» Sarbanes-Oxley Act of 2002

Is Security Awareness Training Worth the Investment?

Every independent and anecdotal investigation into the return on investment of security awareness training shows positive and significant returns, even given the labor costs necessary to complete the courses. Analyst firm Gartner states that an applied example would easily justify why an organization would provide awareness training. According to their data, untrained users click on 90% of the links contained within emails they receive from mail addresses outside the enterprise, resulting in 10,000 malware infections. By their calculations, the infections lead to an overall loss of productivity of 15,000 hours per year, which, at a cost of 15,000 times $85 (average wage), equals $1,275,000.[6]

"After training, users will click one-third fewer of the links contained within emails they receive from mail addresses outside of the enterprise. This results in a 75% decrease in malware infections, to 3,750 - leading to a 40% reduction in loss of hours of productivity (9,000). Intrusions amount to a cost of 9,000 times $85 (average wage), totaling $765,000. The training saves $510,000."[6]

Jeremy Koellish, COO at TekTegrity, Inc., a premium managed IT services company, understands first-hand how security awareness training can open the eyes of senior management. When TekTegrity conducted their first wave of phishing simulation tests, they found their failure rate to be approximately 18%. After two or three rounds of training, they saw the rate drop to a much healthier 3%. Moreover, TekTegrity integrated security awareness training as a core component of their security solution for their customers, and reports similar results across their entire client base.

Best Practices for Effective Security Awareness Training

At the end of the day, the success of security awareness training boils down to the participants; thus, training programs should be designed with employees at center stage. Organizations understand that security awareness programs can make a huge impact, but with the caveat that security operations professionals must conduct programs with the following best practices in mind.

» **Transparency**

When a business launches security awareness training, organizations should clearly communicate the objectives to their teams. This is an opportunity to underscore the value of the training and emphasize that every employee should consider themselves an essential part of the security team. The initial goal of security awareness training is not just to obtain statistics, but rather to raise awareness to the entire organization. And when statistics are collected and shared, it changes perceptions and helps the entire organization grasp the importance of the training.

» **Executive Sponsorship and Buy-in**

Security awareness training cannot be implemented without cultural buy-in from entire organizations, top to bottom. Without budget approval, enforcement, and prioritization, most programs fail. Gaining the support of an executive sponsor should be top priority, and when introducing programs, ensure that communications to the team originate from a company leader to ensure everyone understands the need and respects the importance of the training.

» **Engaging Content**

From a user perspective, relevance is a key contributor to the effectiveness of security awareness training courses. Engaging, interactive courses that relate to real-life experiences are powerful teaching tools. Research indicates that stale, lengthy, or unengaging content reduces the efficacy of training courses. Training fails when it lacks interactive elements, such as gamification or user involvement, and when it panders to fear or is too trite for its users. These learning experiences must be useful on all levels, and should incorporate the cues we all use to learn and retain valuable information. What's more, administrators should always have the ability to evaluate end users on their retention with measureable interactions.

» **Phishing Simulations**

Sending simulated phishing emails to your employees is a reliable way to learn how many are likely to take the bait. These tests resemble real-life scenarios users may face, both at work and in their personal lives. The first emails should be very basic, using your internal style and topics-a performance review or bonus increase, for instance. A standard phishing-style address should be used, rather than an internal address. Subsequent simulations should become more sophisticated and personalized, and tailored to industries and departments. These tests allow security teams to assess which employees simply click through without scrutinizing the sender, while gathering overall statistics on testing failures.

[6] Gartner. "How to Gain Support for Your Security Awareness Program." (January 2017)

Test administrators should focus on detection and reporting clicks, rather than just prevention rates. Phishing response plans should:

- Empower users to report "phishy" emails to IT or security teams
- Ensure users are able identify phishing recipients and recall email details
- Detect phishing recipients who clicked a link or opened an attached file

» **Continuous, Frequent Training**

For a security awareness program to succeed, continuous and frequent monitoring and training capabilities are key. Phishing simulations should be conducted at least once a month, with quarterly or yearly mandated security courses. To improve performance, weekly phishing simulations should be performed, with monthly training courses. Plus, as new employees come on board, security awareness training should be a requirement of onboarding processes.

» **Identifying Offenders**

In every company, there are weaker links in the cybersecurity chain. It's important to identify who they are through testing and other factors, such as their role in the organization. For example, Finance and Sales departments are typically responsible for pertinent financial information; therefore, hackers looking for money will specifically target them through spear phishing techniques, which are routinely sophisticated and personalized. Once you've identified these employees, ensure training is introduced or increased.

Essential Components of Security Awareness Training Solutions

Effective security awareness training starts with learning management software (LMS) and phishing simulations that allow administrators to easily select, set up, run, manage, track, and report on their security awareness initiatives. Software lies at the heart of any security awareness solution and should include the features and qualities listed here.

» **Greater Adoption through Ease of Use**

One of the most important qualities of an LMS is ease of use, especially when companies are driving adoption across organizations. Administrators should never need to train end users on how to use the learning platform. Training should always just be a "course click" away. Plus, given the modern trend of highly-mobile workplaces, it is important that employees are able to access courses anytime, anywhere, from any device. But ease of use does not just extend to end users. If the administrator struggles with the LMS implementation or application, it hinders the value of the training as a whole.

» **Enhanced Productivity through Integrated Systems**

Security awareness training includes three core components: phishing simulators, pre-built security courses through an LMS, and reporting tools. Security professionals are accustomed to purchasing the phishing simulation piece, course materials, and the LMS separately. However, ideal solutions are bundled together, leading to better integration, familiar contracting, provisioning, and support. Also, the simultaneous use of multiple cybersecurity solutions introduces the potential for operational conflict.

Training should also be easy to integrate with company-wide software (HR systems, CRM systems, etc.), and the ability to leverage APIs is essential so the LMS can communicate with these applications. Moreover, to apply a holistic approach to security, endpoint protection and other security tools should be unified. This provides administrators with a single pane of glass through which they can manage tasks and oversee the training objectives. Integration is also key from a security perspective, as it can facilitate training programs that are tailored to each individual user's risk profile and behaviors.

» **Improved Credibility through Customized Content**

For MSPs or businesses that focus on branding their internal content, the ability to customize and brand security training can greatly increase the credibility of the training over anonymous content.

Additionally, the ability to inject customized content such as current events is key, especially in phishing simulations. For example, phishing emails that refer to a current catastrophe, such as wildfires in California or a hurricane in Florida, and that appear to originate from a relief organization, such as the Red Cross, are extraordinarily effective. These sophisticated simulations keep users on their toes, and train them to carefully evaluate whether an email is authentic.

» **More Flexibility with Full Content Management**

Full content management within the LMS is essential. The ability to upload existing courses, videos, and simulations, as well as link content and users to other hosted content can provide flexibility. For example, many businesses benefit from the ability to manage both pre-test and post-test content, as well as the capability to randomize content, create multiple choice answers, or have test results scored and weighted.

» **Better Assessments with Reporting and KPIs**

Tracking and reporting are essential to demonstrate the value of security awareness training. User progress reports and assessments of content efficacy ensure that every aspect of the training is measureable and end users are accountable. Two essentials KPIs that should be measured are vulnerability and awareness, as successful training programs should decrease vulnerability, while simultaneously increasing security awareness.

» **Improved Purchasing Power and ROI with Competitive Pricing**

Security awareness training should be priced competitively. Along with pricing, MSPs and business customers should balance upfront costs against the ROI from the positively altered user behavior, which reduces infections and prevents costs associated with breaches, such as help desk calls and time spent on remediation and disaster recovery.

» **Satisfying Requirements through Compliance Courses**

If security awareness training is an industry or regulatory requirement, specialized course content for compliance should be available. The goal of courses is to ensure everyone in the organization knows their responsibility as a good cyber citizen, and to ensure security audits are passed.

» More Peace of Mind through Data Protection

Finally, it may go without saying, but the LMS must be secure. Ideally, very little user data (if any) should be gathered or stored within the LMS, and while departmental and user reporting should be available, so too should anonymized reports and aggregations. Content needs to be protected and use of the system to launch phishing simulations or other social engineering attacks should be limited to only legitimate use.

Key Considerations for Business Growth

Security awareness training is a smart investment for MSPs. Delivering integrated and continuous training to users at client sites improves their overall cybersecurity posture, and minimizes remediation time, help desk calls, disaster recovery costs, and other cybersecurity-related tasks for MSPs. If you were able to decrease malware infections by 75% with a security awareness program, as Gartner's data indicated, imagine the number of man-hours administrators and technicians would get back to focus on other tasks. In addition, this proactive approach to security helps MSPs build relationships with customers and improve profitability and trust. After all, there's only so much security software can do if an end user accidentally hands over their access credentials for sensitive systems. When you include end user awareness training in your service offering, you're helping your clients make the most of their IT security budget.

Many MSPs offer security awareness training as an add-on paid service, since the proven value of security awareness as an additional layer of defense against breaches is so high. Others are including end user education as a standard component of their bundled security offerings, alongside antivirus and patching services. In this pricing model, MSPs calculate that the savings from dealing with fewer incidents and service calls after customers have begun leveraging training courses and phishing simulations can actually improve the profitability of their offerings. In either model, both MSPs and their customers win.

No Longer a Nicety, a Necessity

The number of data breaches is steadily increasing year over year. In fact, more than 2,200 data breaches were disclosed in the first half of 2017 alone, exposing more than 6 billion records.[7] Plus, the average cost for each lost or stolen record containing sensitive and confidential information in 2017 was calculated at $141.[8] Given these alarming statistics, it's clear organizations both large and small need to embrace a holistic and proactive approach to security.

Security awareness training has been employed by large organizations for years, but due in part to cost, it hasn't been as commonly used among small- to medium-sized businesses. As we have seen, the need for continuous workforce security training has grown exponentially due to the growing frequency and impact of phishing and ransomware attacks. IT security truly is a shared responsibility in every organization, but it isn't always treated as such. That's part of why some security practices and technologies are no longer niceties, but necessities. Security awareness training-particularly succinct, relevant, computer-based training-is a proven way to arm users with knowledge.

About Webroot® Security Awareness Training

Webroot Security Awareness Training is a SaaS offering and is integrated into our existing web-based Webroot Global Site Manager console. That's the same streamlined console that administers award-winning SecureAnywhere® Business Endpoint Protection and DNS Protection. Security Awareness Training from Webroot makes it easy use and manage your workforce training. Plus, it allows administrators to access and manage a variety of Webroot protection solutions in a convenient, cloud-based location. We offer 12 core security awareness courses and numerous phishing simulations all within our unified platform, as well as advanced reporting capabilities to direct training to those who need it most and demonstrate value to clients and IT decision-makers alike. Plus, we cover compliance for PCI, HIPAA, Finance, GDPR, and more. Moreover, Webroot is the only vendor offering security awareness training for the SMB/MSP sector. To learn more about the benefits of Webroot® Security Awareness Training, visit webroot.com/awareness.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

[7] Risk Based Security. "2017 Mid-Year Data Breach QuickView Report." (July 2017)
[8] Ponemon Institute. "2017 Cost of Data Breach Study." (June 2017