The complete guide to security awareness training

2021

Contents

Introduction

How human-targeted attacks are set to evolve in 2021

The Covid-19 pandemic has posed many security challenges. Businesses around the world have adjusted to working from home and social distancing, while also dealing with new threats posed by cyber criminals exploiting fear and curiosity. Even as companies have dealt with these challenges, traditional cyber threats have been as prevalent as ever, making for an increasingly challenging threat landscape.

Among the major cyber threats, malware remains a significant danger. The 2017 WannaCry outbreak that cost businesses worldwide up to $4 billion is still in recent memory, and other new strains of malware are discovered on a daily basis.

Phishing has also seen a resurgence in the last few years, with many new scams being invented to take advantage of unsuspecting companies. Just one variation, the CEO Fraud email scam, cost UK businesses alone £14.8m in 2018.

Staff working from home are outside the direct oversight of IT support teams, and often struggle to deal with cyber threats and appropriately protect company information.

Failing to update software and operating systems, sending data over insecure networks, and increasing reliance on email and online messaging has made employees far more susceptible to threats ranging from malware to phishing.

While technical solutions like spam filters and mobile device management systems are important for protecting end users, with the number of threats and the multitude of systems and communications through which staff perform work, the one unifying risk factor that has to be addressed to fundamentally improve security is the role of human error.

Why human error is the #1 security threat to your business

Almost all successful cyber breaches share one variable in common: human error. Human error can manifest in a multitude of ways: from failing to install software security updates in time to having weak passwords and giving up sensitive information to phishing emails.

Even as modern anti-malware and threat detection software have grown more sophisticated, cyber criminals know that the effectiveness of technical security measures only go as far as they are properly utilised by humans.

If a cyber criminal manages to guess the password to an online company portal, or uses social engineering to get an employee to make a payment to a bank account controlled by the cyber criminal, there is nothing that technical solutions can do to stop that intrusion.

In 2014, IBM conducted a study into the cyber breaches that occurred among thousands of their customers in over 130 countries. This study was the most wide-reaching look into the causes of cyber breaches that had been performed at that point, but its results have since been corroborated by similar studies.

One of the key findings of the IBM study was that human error was a major contributing cause in 95% of all breaches.

In other words, had human error not been a factor, the chances are that 19 out of 20 breaches analysed in the study would not have happened at all.

"Human error was a contributing factor to 95% of all breaches"

Since human error plays such a vast role in cyber breaches, addressing it is key to reducing the chances of your business being successfully targeted. It also allows you to protect your business from a far wider range of threats than any single technical solution could - and can potentially empower your workforce to actively look out for and report new threats they may encounter.

Mitigation of human error must be key to business cyber security in 2021 - and in the next section we'll look at the best ways to go about it.

When does human error take place?

Two factors have to be present in order for human error to manifest: opportunity and decision. Opportunity means that there is a situation where a human is allowed to make a mistake: for example, letting end users handle software updates rather than forcing security updates through with patch management. Decision is the action of the individual: in this case, the lack of action in installing security updates when they are available.

A comprehensive mitigation effort includes both reducing the opportunity for error as well as improving the decisions made on the part of the end users. Taking action in both areas is essential to ensure that human error is thoroughly addressed.

In the case of patching, for example, a technical measure such as introducing patch management may reduce the opportunity for human error to a minimum in most cases - but it is still essential to account for situations where the technical solutions has a temporary lapse, or if a new situation such as a BYOD policy where users are allowed to use their own devices without patch management is introduced.

In other cases, such as with phishing emails, technical measures such as spam filters and breach detection software have a very limited effect in reducing opportunity for error when faced with a targeted attack. In those cases, the only effective way to mitigate human error is by teaching end users how to make better judgments.

"Two factors have to be present in order for human error to manifest: opportunity and decision"

How can employees make safer everyday security decisions?

1 Understanding

The user has to recognise that they are in a situation where security is potentially at stake. Without recognising this, the user may not even realise that they are making a decision at all through their inaction.

2 Empowerment

The user has to know what the correct course of action is. This doesn't necessarily require the them to completely understand the threat, but often is as simple as reporting the situation to a person in the IT or security department who can look into it.

3 Education

The user must know why security matters, so they understand the importance of not ignoring security procedures and are aware of the potential implications of a breach.

4 Eliminating pain avoidance

Issues such as weak password security and failure to patch software persist in organisations across the world, despite many computer users understanding why these issues are critical to security. The reason that action is not taken despite knowledge is due to what we refer to as pain avoidance. Having a unique and strong password requires more time to create, and more effort to remember, than a short, weak, or reused password.

Despite a user knowing better, this 'pain' caused by creating a strong password is often strong enough to make the user go against their best judgment. This is compounded by the fact that, despite many users taking the correct action under optimal circumstances, busy and urgent work situations, as well as stress, can make security measures feel even more 'painful' to users.

End users have to feel that the pain caused by following security best practices is less than the satisfaction gained by not doing so. Technical measures such as password managers are essential in this, as they make acting in a secure manner far easier: if employees don't have to create or remember their own passwords, they have no reason not to use secure ones.

Simultaneously, the threshold for performing the correct action must be lowered through cultural change. This means putting security at the forefront of decision making, and ensuring that users never feel they are 'wasting time' by taking appropriate security precautions.

Effective security awareness training addresses not one, but all four of these factors. This means identifying situations where data or systems could be compromised, understanding best practices, knowing what the potential consequences of breaches are, and finally helping to push through a cultural change to create an environment where security considerations are always taken into decision making.

Security Awareness at Home

Keeping staff security-savvy when working from home

The global response to the Covid-19 pandemic has caused many changes in workplaces. The change that has had the most significant impact on security has been the transformation of many businesses to having most or all of their staff switch to working from home within a short period of time, which has led to many end users being at higher risk of succumbing to online threats.

Employees that weren't used to working from home before the pandemic quickly discovered some of the issues that it would cause: having to look after children and pets, dealing with poor internet connectivity, and putting up with all the other disturbances that can happen at home. In the midst of all these new changes to the working environment, security too often fell to the bottom of users' priority lists.

End users that work from home are out of the oversight of the IT support department, and may struggle with simple tech-related issues. In addition, essential security tasks like updating software and operating systems, updating router firmware and securing the network, were suddenly placed into the hands of end users.

It's no wonder that cyber criminals haven't wasted a second in exploiting the circumstances of the pandemic to come up with new forms of scams and cyber crime.

In the midst of all these new changes to the working environment, security too often fell to the bottom of users' priority lists.

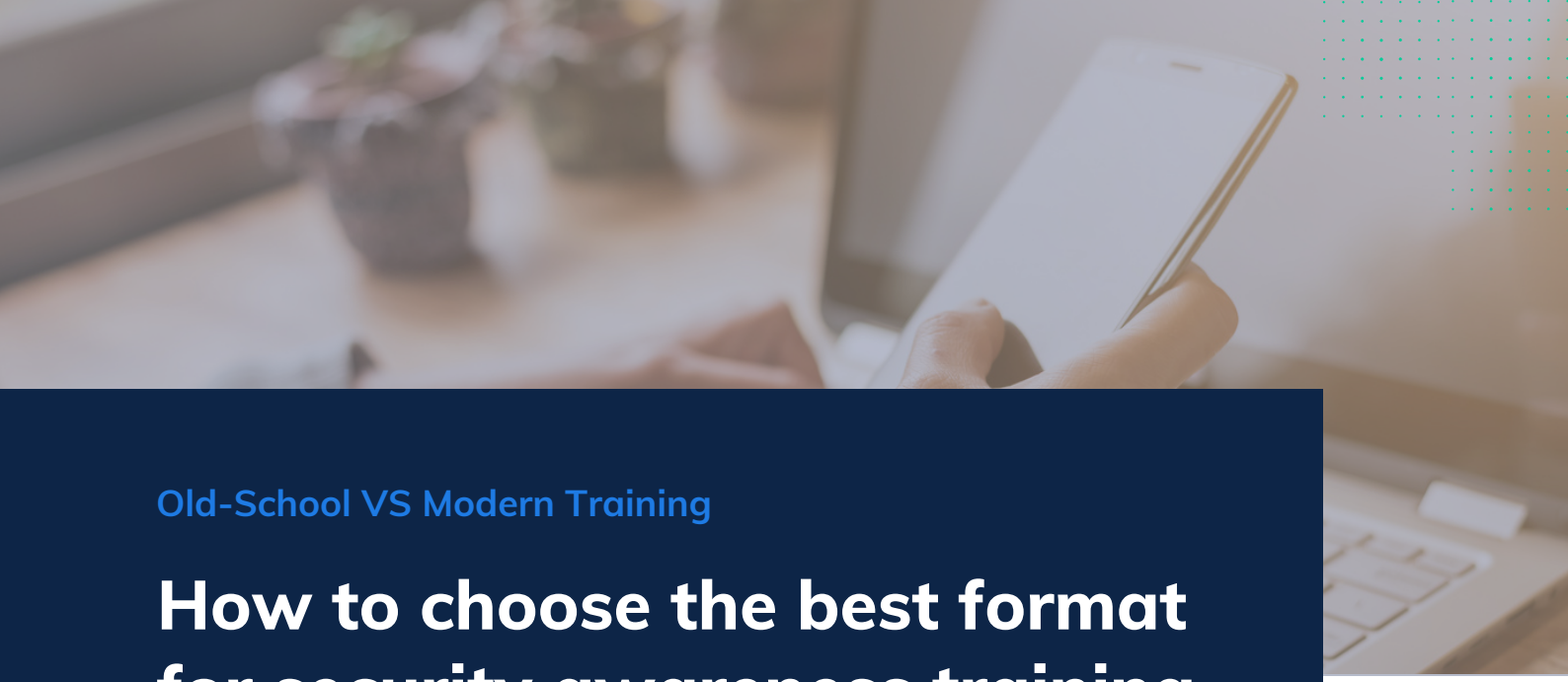
How to address security when end users are at home

The IT support team can't be at every end users' home, which is why it is essential to ensure that, in addition to having the right equipment, end users are aware of their individual responsibilities in keeping up security. End users need to know that they are responsible for ensuring that they only access company information and networks on devices and networks that are up-to-date and secure.

Security awareness training is key to ensuring that end users know how to keep up security. It's best to break up training into small, digestible components, as this ensures that users aren't overwhelmed. Training should also take place regularly - once a month, at the minimum - to ensure that key learning is retained, and that users won't forget about security as soon as the next work project comes along that shakes up the list of priorities. Lastly, it is important to test end users.

It should be made clear that this isn't for judging or penalising users who struggle with their training, but rather to identify key security gaps across the workforce, and address these before they can be exploited by cyber criminals.

"Security awareness training is key to ensuring that end users know how to keep up security"



Old-School VS Modern Training

How to choose the best format for security awareness training

Security awareness training isn't all one and the same. The way in which training is performed, structured and presented will have a major effect on its effectiveness in genuinely improving security outcomes in your organisation. In this section, we'll take a look at what exactly is the best way to perform security awareness training for your end users.

Security awareness training used to mean making end users sit through an annual session consisting of hours of lectures and slideshows. The idea was that users would remember something of what they saw and heard - and in the worst case scenario at least the box for 'educating users' could be ticked. How did it far in actually improving security outcomes though? It didn't work, and everyone hated it.

Why yearly 'tick-box' training fails miserably

There are a number of reasons why this type of annual lecture-based training isn't effective.

The first of these is that in an annual training session, there will simply be too much information at once for any employee to digest and remember.

Even if users are given learning material to take with them or are sent occasional reminders, chances are that most of the material in the training session will go in through one ear and out the other - forgotten in mere moments.

Lectures and slideshows are simply not engaging formats for end users to learn from. They fail to raise the interest of employees in the same way that video and interactive content do, and too often are filled with unnecessary information that isn't relevant to every end user.

Slides filled to the brim with small text are sure to make any employee fall asleep halfway through the session.

The final, major reason why traditional training isn't effective is that it doesn't make use of learning through repetition. If there is a year between learning sessions, users simply won't remember what they've learned - and awareness of security issues in general will plummet in the days and weeks after training. Security can't be a one-time thing, but must be year round in order to be effective.

Security awareness training has increasingly shifted to online software-as-a-service solutions. Cloud-based training offers some immediate benefits over traditional methods, but isn't necessarily the ultimate answer to security awareness unless it delivers in certain areas that are essential for genuinely improving security outcomes.

How to make modern training truly effective

Breaking down material

There is a limited amount of information that a person can absorb at a time. In order to not overwhelm end users, training should be broken down into segments, each with their own clear, simple message that's presented in an easily-digestible fashion.

Continuous learning

Breaking down learning material also allows learning to easily be made continuous, rather than a one-time thing, and allows courses to be sent out regularly throughout the year - helping keep security awareness consistently on the minds of end users, as well as improving learning retention.

Relevant material

When an end user is given information that they feel is not relevant to them, they will quickly start losing interest and paying less attention. Learning material needs to not only avoid jargon and technical terms, but be made with real-life situations in mind that the end user could encounter.

Embed security into your culture

Training has to be a part of a business culture where security is always given the consideration it needs, and users are encouraged to bring up concerns and ask questions.

Practical advice

It's essential that employees walk away from training with actual steps in mind that they can put to use right away in their daily work activities. Giving employees the chance to put their training to test right away also helps build memory - and can be achieved using tools such as phishing simulation.

Video and interactive content

Video and interactive content are great for engaging users who may prefer a different type of learning experience. Many people learn by doing, answering questions or otherwise taking part.

Measuring the impact

It's essential that, after training sessions, users are tested on what they've learned. This helps you know that users are walking away having learned something - but also helps the learning process of users as they recollect the information they have just learned from their own memory.

Building a Security-Savvy Culture

How to embed security into everyday staff culture

Security awareness training will not be effective in improving security outcomes if it is not accompanied by cultural change. Comprehensive training will teach end users how to recognise situations where security is at risk and how to deal with them appropriately - but this knowledge is not going to be put into practice unless the user feels that security is valued in their culture.

With the growing number of threats present, as well as the increasing complexity of business services and access to data and systems from mobile devices, it is impossible to know where the next threat or accidental leak to your business might appear.

This is why security shouldn't be about ensuring that your end users choose strong passwords or follow other specific steps - but rather about empowering them to be active guardians of your business, its systems, devices and data.

"Comprehensive training will teach end users how to recognise situations where security is at risk and how to deal with them appropriately - but this knowledge is not going to be put into practice unless the user feels that security is valued in their culture."

How to build a security-savvy culture

Getting C-level support

Cultural change and the company's values have to come from the top. Senior management has an important role to play in emphasising the role of security in the business - but it is essential that they grow, rather than dictate, the new culture.

This means encouraging employees to take an active role by asking them to bring up concerns relating to their own roles, and prompting them to ask questions and become engaged with security issues. This way, users feel like they are involved in the security process, and start actively thinking about the security considerations in their own roles.

Least privilege access

While the principle of least privilege is often seen as a technical measure - limiting each user to only the privileges that they require for their specific duties - it should also be embedded directly into corporate culture.

This means encouraging users to actively report when they have access to more data or systems than they need - helping to limit possibilities of breaches.

Physical security

In terms of physical measures, items like posters can be helpful in building a security culture, and also contain helpful reminders on topics such as password strength.

It's important to remember though that just sticking a poster on a wall won't achieve anything by itself, but they should be used as starters for discussion, or serve in complement to training material that users are already engaged with.

Essential Training Topics for 2021

What are the essential training topics for 2021?

While each organisation and each job role will have different requirements, there are some essential areas that are worth ensuring every single end user is aware of.

Top topics for 2021:

1. Phishing Techniques
2. Social Engineering
3. Security at Home
4. Secure Internet & Email Use
5. Working Remotely
6. Mobile Device Security
7. Password & Authentication
8. Cloud Security
9. Public Wi-Fi
10. Physical Security
11. Removable Media
12. Secure Social Media Use

#1. Phishing Techniques

Phishing remains a huge threat. One of the reasons why phishing is so popular among cyber criminals is that it can be easily customised to make use of any event or circumstance - such as the Covid-19 pandemic - to target users with new scams. Template-based scams offering information to victims have become more popular than ever - while spear-phishing attacks that target individual users and businesses remain the most dangerous kind.

End users are most susceptible to phishing emails that create a sense of urgency or offer something valuable to the user. It's essential to train end users to double-check that they can trust who an email is from before clicking links or giving up information. While it's impossible for users to catch every phishing email, security awareness combined with spam filters ensure that the potential reach of phishing emails is limited to the minimum.

#2. Social Engineering

Phishing is only one of many types of social engineering attacks. Physical and phone-based social engineering attacks are also used by criminals to gain access to secure premises and sensitive data.

It's essential that employees are educated on the different types of social engineering attack - from those over the phone to in-person threats - and understand how to properly deal with any potential offender.

#3. Security at Home

Working from home was raised to the forefront of end user security in 2020, as businesses across the globe encouraged staff to switch to remote working. The speed of this transfer meant that many users were left ill-equipped with tools and knowledge to ensure that they can carry out their work securely.

It's essential to train any employees working from home how they can ensure that the company's data and network aren't compromised through remote access. Updating software, protecting Wi-Fi networks, and using security tools such as VPNs to ensure secure access have become an essential part of end user training.

#4. Secure Internet & Email Use

In 2021, it is a rare employee that doesn't use the internet or email at work. While the pandemic has made businesses more reliant on the internet than ever, use of the internet also carries security risks. Users may inadvertently install malware, leak data, give up credentials to phishing emails or fall for any of the many other attacks that cyber criminals are targeting them with.

Training users to use the internet and email securely is essential. Most of this comes down to awareness: knowing that emails can cause data breaches if sent carelessly, and that malicious sites can contain malware.

There should also be practical advice in training, such as informing users about the difference between cc and bcc fields, and what the HTTPS encryption symbol on websites means.

#5. Working Remotely

In 2021, remote work is going to be more popular than ever. While the pandemic has given a jump-start to home working in many businesses, it is likely to continue beyond the pandemic. Employees have started to get used to working from home, and businesses are realising its benefits.

Working remotely also carries risks. Laptops, mobile phones, tablets and other devices can pose a serious security threat if they are lost or stolen. If employees store or access company data from their mobile devices, this data all becomes vulnerable if a device falls into the wrong hands. When educating users on secure remote working, focus should be placed on helping users identify points where systems or data could become compromised - and the steps they can take to mitigate these risks.

#6. Mobile Device Security

Mobile device use in businesses has been growing quickly, and in 2021 this trend is expected to become even more widespread than before. Mobile devices such as laptops, mobile phones and tablets allow employees to work from home, coffee shops, while travelling or just about anywhere they wish, providing flexibility to both themselves and the business. As convenient as mobile devices are, they do come with risks that users must be educated about.

Users should be educated on how mobile devices can potentially expose company data and systems to unauthorised access. This involves access through lost or stolen devices, as well as malicious software and illegitimate third-party apps.

#7. Passwords & Authentication

Passwords continue to be a major headache for businesses, employees and customers alike. Humans simply aren't designed to remember long, complex phrases - especially not dozens of them. This means that employees are constantly tempted to take the easy way out and make them easy to remember - especially when they are required to share access to apps and services with their colleagues.

The majority of end users will be aware of why password security matters, and have the basic gist of what makes a strong password. The focus on training around passwords and authentication should be on focusing practicable advice on how to keep up password security without making life harder for your end users. This means encouraging the use of password managers (if this is something your business permits), asking employees to turn on two-factor authentication for all services and systems with access to sensitive data, as well as teaching employees how to make a password that is both reasonably complex while being reasonably easy to remember.

#8. Cloud Security

Over the last few years, business services and data have increasingly shifted to the cloud. In 2021, this trend is coming to culmination, with many business operations being conducted entirely using web-based tools and services. While the cloud offers great flexibility to businesses, it is essential that users know how to use and access it securely.

Strong passwords and authentication, as well as email security, become of extra importance when your business uses cloud services.

A bad actor that guesses an employee's passwords could access your sensitive data from anywhere in the world, which is why it is essential that employees are educated on the measures necessary to keep cloud accounts secure. Multi-factor authentication is especially a must for all services and apps that contain sensitive business data.

#9. Public Wi-Fi

As users increasingly work while on the go, chances are that they will connect to business services, networks or data from public Wi-Fi access points. Public Wi-Fi is highly convenient for mobile work, but also comes with security risks.

It's important to teach end users that their data could potentially be intercepted on public Wi-Fi networks. If you allow your end users to access company data or services through public Wi-Fi networks, you should equip them with Virtual Private Network software and educate them on using it in a secure manner.

#10. Physical Security

Even as cyber security threats multiply, it is essential that physical security is not overlooked. It is no use protecting data with strong passwords and multi-factor authentication if an unauthorised person can simply walk into the office and pick up a paper copy of a sensitive document right off the printer tray.

When training end users in physical security, it is essential that focus is placed on identifying and mitigating threats relevant to individual end users' day-to-day activities. If your business is based in an office, every employee is going to walk through the office door - so tailgating is an example of a security threat that is relevant to all employees. End users should be trained to actively think about what areas and documents are secure, and ensure that they are always locked securely or accounted for when not in use.

#11. Removable Media

Even as file sharing and online collaboration services on the internet have become more popular, removable devices are still seeing widespread use in businesses. As useful as removable media devices are, they pose many risks: they are easily lost or stolen, potentially leading to compromise of data, or could be replaced with devices containing malware. A common scam is leaving a virus-infected USB drive in an office parking lot, waiting to be picked up and inserted into a company computer by an unsuspecting employee. In addition, many users are unaware that it's not only storage devices that could pose a risk: even simple USB or charging cables could be modified by a cyber criminal to contain malware.

Educating end users about secure use of removable media comes down to accountability. It should be made clear to users that they have to take responsibility for devices that are under their control - and that they should not plug in any devices that have been unaccounted for into any computer, but instead report them to the IT team or to security personnel.

#12. Secure Social Media Use

Employees - and businesses - spend an increasing amount of their day on social media. It is essential, however, to ensure that the business' security won't be compromised over careless use of social networks.

Focus on social media training should be placed on making users aware that what they share might be available to anyone on the internet - and that even small details from within the office could be crucial to attackers. For example, an innocent selfie from within the office could show a whiteboard in the background with sensitive business information, or even a customer's details.