GRIT TECHNOLOGIES

THE WHYS AND HOWS OF AN ENGAGING

CYBERSECURITY AWARENESS TRAINING PROGRAM

TABLE OF CONTENTS

Why is it crucial for SMBs to have a cybersecurity training program?

Every modern business utilizes the internet to carry out various tasks, from sending teamwide emails to updating the company website to receiving online payments. In the past year alone, we've seen a stratospheric surge in internet usage, as the pandemic compelled businesses and other institutions to adopt cloud technologies to maintain operations.

But while the internet is essential in keeping day-to-day operations going, it also poses a host of cybersecurity risks to small- and medium-sized businesses (SMBs). Left unaddressed, these security risks can shut down your business for good.

The reality of cybersecurity today

The internet is swarming with millions of viruses, malware, and other security threats that can compromise your cyber defenses. The following statistics can help you gain a better understanding of how serious the cybersecurity landscape is.

- **66% of organizations experienced targeted phishing attempts in 2020** (Proofpoint's 2021 State of the Phish). Phishing is a social engineering scheme, which means it relies on the manipulation of human emotions to carry out a cybercrime. In a phishing attempt, a phisher sends out an email purporting to be from a trustworthy entity, and then lures the victim into divulging sensitive data, such as their username and password combination or their credit card information. Because of the seeming legitimacy and clever execution of phishing emails, phishing is one of the most successful cyberthreats today.

- **43% of cyberattacks were launched against small businesses** (Verizon's 2019 Data Breach Investigations Report). It's a common misconception that online criminals only target big corporations, as these enterprises have more data that can be stolen or sold in the black market. In reality, malicious actors sometimes prefer attacking SMBs because these businesses generally don't have a robust cybersecurity strategy, making them easy prey.
- **85% of data breaches involved the human element** (Verizon's 2021 Data Breach Investigations Report). Threats have grown more sophisticated over time, and recently, the ill-intentioned have found a way to get through cyber defenses without hacking systems. They instead send emails to unsuspecting staff and rely on the latter to click on a malicious link or download a compromised file. Not only does this approach take less effort, but it is often more successful. This also means that every internal user — from your intern to your CEO — is a target who can be a victim of a cyberattack.
- **34% of data breaches involved internal actors** (Verizon's 2019 Data Breach Investigations Report). Hackers are not the only ones who can compromise your data. Sometimes, the threat comes from within your ranks. Risk could stem from a vengeful employee who leaks company data to your competitors or a remote worker who uses the same device for both work and personal tasks. Whether they intentionally pose cybersecurity risks or not, internal threat actors exist and shouldn't be taken out of the equation when planning for a holistic data security strategy.

Strengthening cyber defenses through security awareness

SMBs cannot remain complacent with their cybersecurity. It's clear that they are attractive cybercriminal targets, so they must do what they can to strengthen their defenses and keep threats at bay. An impenetrable cybersecurity strategy follows a three-pronged approach that involves implementing controls around the core pillars of an IT infrastructure: people, processes, and technology. A cybersecurity awareness training program strengthens the first pillar — people.

With over 8 out of 10 data breach attempts relying on human error to succeed, SMBs must develop a program that will educate staff on risk management and teach them the best practices in keeping data secure. Anyone from your company can unwittingly become a victim of a cyberattack and expose your systems to malicious actors, so don't let the human element be your weakest link. Beef up your defenses by creating an engaging cybersecurity awareness program.

What you need to know about cybersecurity awareness training programs

The goal of a cybersecurity awareness training program is to equip employees with the proper behavior and skills which will allow them to be less of a threat to the business's overall cybersecurity posture. When your workers know how to navigate the web securely and are able to recognize, manage, and report cyberthreats that they encounter, they are less likely to fall victim to the different schemes cybercriminals employ.

Specifically, security awareness training helps organizations:

- ✓ Enhance overall business resilience against cyber risks
- ✓ Shift employees' mindsets and change their behavior to develop a culture of cybersecurity
- ✓ Demonstrate compliance and improve/maintain audit results
- ✓ Minimize human error and mitigate security risks

Cybersecurity awareness training should not be a one-time event; instead, it should be conducted regularly and woven into the company's culture. The onboarding process, for instance, can include introductory cybersecurity topics, such as managing passwords and dealing with spam emails.

The cyberthreat landscape is also evolving by the second, so be sure to update your cybersecurity strategy based on the most recent information. Regularly training employees on salient cybersecurity developments is imperative, as this allows them to keep abreast of the tactics malicious actors use, empowering your workforce to be more effective at mitigating threats.

However, because every company is unique in terms of industry, size, culture, and technology use, there is no one-size-fits-all approach to creating an effective cybersecurity awareness training program. How you design your program will depend on several factors, including your organization's security needs, existing IT infrastructure, and employee cybersecurity knowledge. But while no two cybersecurity awareness training programs are exactly alike, their success relies on one key element: **employee engagement**.

The importance of engagement in cybersecurity training

Your workforce can make or break the security of your organization. It is vital that every single one of your employees understands and is able to carry out their role in preventing, reducing, and mitigating cyberthreats. If someone slips and commits just one tiny error, all your other technical security measures can be rendered ineffective. This is why you need engaged employees who are prepared to go the extra mile in protecting your organization.

Employee engagement refers to the staff's level of commitment, passion, and effort about their work, and, consequently, the organization to which they belong. Employees with high engagement are more likely to support initiatives by their company, such as those related to cybersecurity.

If you can keep employee engagement up, there is a higher chance of generating employee buy-in and developing their commitment to the company's cybersecurity strategy. And when your cybersecurity awareness training engages your employees, it can turn apathetic users into advocates of cybersecurity.

6 Ways to make your cybersecurity awareness training more engaging

A cybersecurity awareness training program is a series of activities designed to orient employees about the specific actions they can take to prevent a cyber disaster from happening. Conducting an effective cybersecurity awareness training program has many benefits, including reduced cyber risks and better compliance preparedness. However, creating an engaging cybersecurity awareness training program is often easier said than done.

Make your training more effective and meaningful by incorporating the following strategies:

1. Gamify your training.
2. Make the training feel natural.
3. Make it relevant and up to date.
4. Learn from your employees.
5. Leverage learning by experience.
6. Set realistic goals.

1 Gamify your training

Gamification is a technique often used by marketing teams to encourage engagement with a service or product. Essentially, to gamify something is to apply to it the elements of game playing, such as scoring points, undergoing challenges, and getting special rewards.

You can gamify your cybersecurity awareness training program in several ways. For instance, you can set up a reward system where people who display positive cybersecurity behavior are incentivized.

You can give out cards that will be stamped every time an employee reaches a security milestone; for example, they get a stamp for the 1st, 20th, and 100th email they send without security risks. Then, after reaching a certain number of stamps, they can claim a gift certificate, voucher, or other types of rewards.

You can also host a cybersecurity obstacle course with various “stops” consisting of questions and activities related to data protection. It can be a friendly competition among team members, and the first person who reaches the finish line can pick a reward from a pool of prizes. Not only is this an effective way to encourage people to stay vigilant, but it also makes employees appreciate the company's recognition of their efforts to be more aware of cyber risks.

2 Make the training feel natural

If you only conduct cybersecurity training once or twice a year, your employees might perceive it as an inessential annual event that can be skipped. Consequently, they might view cybersecurity responsibility as an occasional, nonurgent task that doesn't have to be followed strictly outside of the training period.

Instead, strive to build a culture of cybersecurity in your business by incorporating company-wide cybersecurity-related activities, tasks, and updates. Send regular virtual newsletters about the latest in cybersecurity, or dedicate a few minutes of your week to briefly discuss the security incidents your staff have encountered recently. If you have a distributed workforce, hold a series of Zoom meetings to talk about the security risks of remote working and the steps your team can undertake to protect data in such a setup. Conducting these kinds of activities makes cybersecurity a regular part of your staff’s work life and always keeps them on their toes.

When cyber responsibility feels natural to your employees, it doesn’t get in the way of them doing their tasks. In fact, they will better understand the need to be constantly vigilant of cyberthreats, whether they are checking their emails, browsing the web, or communicating with colleagues

3 Make it relevant and up to date

Constantly hearing about cyberattacks on large corporations or those that take place on the other side of the world may not pique your employees' interest. They may even think that they're untouchable when it comes to threats. To engage participants, discuss cybersecurity in a way that will make the concept feel real and immediate. For instance, if you're a healthcare practice in Michigan, use cybersecurity incidents from your industry and location as springboards for discussion. Center on authentic experiences that your staff can relate to, as doing so will make them realize that they have something at stake in protecting company data.

And because cyberattack schemes are always evolving, your training should take into consideration the changes in the technology landscape. Regularly review your objectives, training materials, and teaching approach to make sure that these are up to date and accurate. Avoid recycling or repeating images, as people tend to skip over them after a while, thinking that they already know what's written on them even if you've actually updated some figures or rolled out a new campaign.

4 Learn from your employees

Most of your employees probably already have an idea about good cybersecurity practices. A good percentage of your workforce may even have already encountered spam, phishing scams, or websites with malicious ads. Employee knowledge and experiences matter when it comes to protecting your data, so consult with your staff to find out what they already know and what they don't. Knowing your workforce's level of cybersecurity awareness will help you identify the weakest links in your security posture and make sure that you're addressing all the security gaps.

What's more, getting input from participants will make them feel appreciated. Your staff will be more engaged in the training if you don't make them feel undervalued. For instance, teaching them things they already know may seem like you're talking down to them. Your workforce is integral to your data security, and your training should make them feel empowered.

5 Leverage learning by experience

One of the goals of cybersecurity awareness training is to equip participants with skills they can use in real-life scenarios involving cyberthreats. Because of this, training programs should include activities whereby employees learn by doing and reflecting on their experience.

When planning your program, make sure that you include hands-on activities that will enable your employees to connect the theory of cybersecurity to its practice. A simulated cyberattack under a controlled environment, for example, can better prepare your staff for the real thing. After a session on the most common tactics phishers use, you can conduct “live fire” training exercises where you deliberately try to phish people in your company. Or, after discussing the merits of using a virtual private network (VPN), you can ask your participants to observe the change in their IP addresses before and after they connect to a VPN client.

6 Set realistic goals

Every company wants to secure its data and prevent a breach. However, achieving robust cybersecurity is not an easy feat. Conducting cybersecurity awareness training will not turn your employees into cybersecurity experts overnight. This is why it’s important to set realistic goals; if you go all out with your cybersecurity training, you might overwhelm employees and lose engagement.

Aim for results that are attainable, measurable, and impactful. Set objectives that will gradually let people get closer to goals, and try not to implement all security measures at once. You can start with basic training topics, like how to filter emails for malicious content, then gradually move on to more advanced issues, such as how to identify and handle a voice phishing scam.

There is no way to fast-track cybersecurity awareness. Continuously assess your staff’s learning pace so you can recalibrate goals if necessary. Be sure to give your staff enough time to get to know their role in data protection and form habits that positively impact the company’s overall cybersecurity posture.

Tools you can use for your cybersecurity awareness training program

While GRIT is committed to helping you solve technological challenges, we also recognize that your business hurdles cannot be solved solely by technology. This is why we offer a wide range of solutions that cover all the bases. Not only do we have managed IT services that can help optimize your tech infrastructure, but we also have business process improvement services for those looking to streamline operations. We take a look at the bigger picture where technology, processes, and people work together to drive your business forward.

When it comes to cybersecurity, we believe that a robust cyber defense takes into account the way people work in practice, and that security shouldn't get in the way of people getting their jobs done. In fact, the opposite should be true: the best cybersecurity defense improves processes and benefits the workforce.

Your employees can be your most effective resource in preventing and detecting security incidents if you invest in their training and create a company culture that encourages them to practice good cybersecurity habits. This is why you should look into solutions specifically designed to train people in cybersecurity. If you have a tight budget, there are free tools in the market that cover cybersecurity basics. However, if you want to make the most of your investment, you can seek the help of organizations that specialize in cybersecurity awareness programs. Most of these organizations will have intelligent business solutions that will allow you to:

- → Conduct baseline testing to assess your employees' existing cybersecurity awareness levels; for instance, their propensity to being phished.
- → Utilize a wide array of security awareness training content, including posters, newsletters, interactive modules, videos, games, and automated campaigns.
- → Simulate cyberattacks to phish your training participants. Some even allow you to choose between launching a fully automated phishing attack or selecting a scheme from thousands of phishing templates to customize the attack and make it more convincing. Most attack databases also have tools that monitor which and how often employees fall prey to certain attacks.
- → See the results of your cybersecurity awareness training, complete with enterprise-strength reporting, statistics, and graphs so you can measure the success of your investment. You can use these results to further modify and customize your cybersecurity program to make it more effective.

Need a hand with setting up or improving your cyber defenses?

We are your reliable IT support and managed services provider in Michigan, offering complete and efficient cybersecurity solutions that minimize risk so you can focus on achieving your goals. Whether you want to overhaul your cybersecurity infrastructure or simply upgrade your existing solutions, we can provide you with a wide range of customized tools that will strengthen your cybersecurity posture.

CONTACT US TODAY TO FIND OUT MORE!

Phone: **Detroit 586.286.8324/ Grand Rapids 616.251.1117** Email: **info@grittechs.com**

GRIT TECHNOLOGIES

www.grittechs.com