How to Conduct Awesome Cyber-Safety Training

in 30 minutes or less without boring your team

A STEP-BY-STEP GUIDE

Conducting security awareness training? This step-by-step guide will help you even if you're starting from scratch

The Author

HELLO THERE! I'M SUE RICHARDS.

Known as “Suecurity”, I have the experience of building world-class Information Security programs from the ground up. My superpower lies in transforming security awareness training from concept to hosting fun, social experiences that I call Securi-TEA parties.

I completed my Masters in Information Technology/Information Security at Lipscomb University. As a Certified Information Security Manager (CISM), I have the proven expertise in Information Security policy, governance and risk strategies. I use various models for conducting risk assessments and compliance readiness assessments for clients in a wide variety of industries.

Today, I beat the hackers at their own social engineering game by making security awareness both fun and informative. I can help you breathe new life into your security awareness training program too.

MORE ON SUREIT.WORKS

CHAPTER 1

3 biggest mistakes Security Awareness programs make

SureIT

3 biggest mistakes of traditional security awareness training programs

1. BORING AND CONFUSING CONTENT

We have all had to suffer through boring security awareness training sessions. The never-ending slide deck using jargon like ransomware, multi-factor authentication, vulnerabilities, URL, zzzz, Who needs to know what a URL means?

Hackers use specific techniques to get unsuspecting people to click on links, share private information and even give them physical access to office spaces. Traditional security awareness tries too hard to cover everything all at once and it's confusing.

2. INFREQUENT

Most organizations conduct security awareness training just once per year. Some more savvy companies may train once per quarter, but hackers are trying every single day to gain unauthorized access to your systems and data.

We listen to podcasts on our daily drive to or from work. We absorb information in small snapshots.

Who sits down once per year to learn something without the ability to review and apply it more frequently?

It's understandable that security awareness isn't effective if it is limited to infrequent sessions.

3. NOT RELEVANT

Your organization and team culture is unique. What may resonate with one group may not resonate with other industries.

For example, those in the dental field can relate to good oral hygiene. They work dilligently with their patients to instill good hygiene practices. Security awareness training that leverages this basic tenant of a thriving dental practice will work great in one setting. Using those principles or examples may not resonate as well in a bank or other financial institution.

You know your business and your security awareness program should be tailored to you.

CHAPTER 2

5 ways to fix those mistakes fast

SureIT

1 Mix it Up

Choose a wide variety of ways to include security awareness training. Instead of relegating it to one boring video training per year, send out newsletters, post to the company intranet, and get out and talk with your teams.

Ask to be included in the next town hall or monthly staff meeting. Give a quick 5 minute talk about security incidents, physical security tips or hacking schemes you've seen in the news. If your organization uses chat like Slack or Telegram, add a Security Awareness channel and post timely content, memes and stories to keep security awareness embedded in the day to day culture.

2 Fit your Industry

Your organization's culture is unique, even within your industry. Make sure you tailor the security awareness training for how your company works. For example, focusing on physical security is different for remote workers than it is for those who work together in a physical building. Securing customer data is still paramount no matter the setting. If you are training remote workers, make sure they follow a clean desk/ clear screen policy at home.

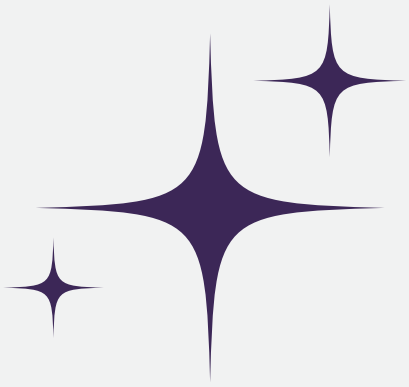
Don't spend a lot of time on HIPAA regulations if your industry is not healthcare. Also be sure to review any local or state compliance requirements and incorporate these regulations into your training program. If you're not sure what is legally required check with your legal counsel as you build your program.

3 Make it Fun

There are lots of ways to incoroporate security awareness that don't stretch your budget.

Work with your People team to find time on the company calendar and incorporate games, puzzles and contests with a cyber-aware mindset.

Tie in seasons like vacation time for travel tips, shark week for email phishing or seasonal holidays to remind people that hackers never take a holiday.



SOME FUN IDEAS

Create a contest, a crossword puzzle or word search and give away a small prize for anyone who completes it.

Set up a competition between department leeaders to reward the team or group with the most participation.

Create an "unsecure workstation" and show sensitive information left out on the desk or thrown in the wastebasket. Include a post-it note with "PASSWORD" written on it on the monitor. Surround the unsecure workstation with yellow tape to get attention, and have team members spot all the security issues.

4 Find Advocates

Seek out people on various teams who understand security awareness and give them extra time and attention. They can be advocates for you. If someone on their team isn't sure if a link is valid, instead of asking you, they can turn to the "security maven" on their team.

Equally important is to get buy in from senior leadership. The tone at the top really does make a difference when implementing an effective security awareness program. Spend time with senior leadership and talk in terms they understand. Have solid facts and figures in the cost of a breach vs. your budget.

5 Bring it Home

Making it personal and describe how information security can be implemented at home. People want to keep their family safe, so include tips to help when kids go back to school, when familiies travel on vacation or staying safe at the holidays.

Talk to your teams about how hackers are targeting the elderly and how social media posts can put them at risk.

MEMES

A picture and slogan in the form of a meme can help illustrate an idea. Read on in the case studies to see some examples.

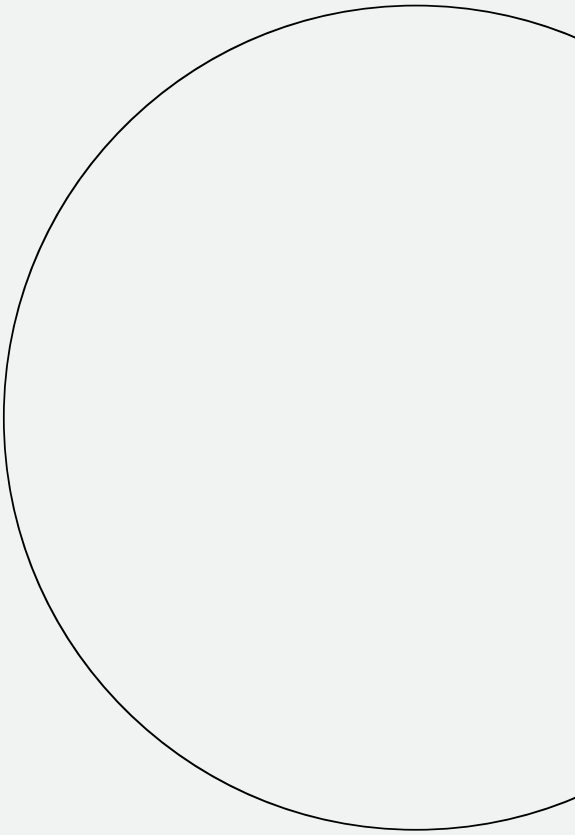
CHAPTER 3

Start your cyber-safety training program

SureIT

How to Start your Training Program in 5 steps

1. DETERMINE YOUR BUDGET
2. KNOW WHAT IS REQUIRED
3. GATHER YOUR CONTENT
4. PLAN YOUR PROGRAM
5. LAUNCH



1. DETERMINE YOUR BUDGET

When you know your training budget, you can use the funds to plan all kinds of fun training programs. Work with senior leadership and your People team to see what training platforms may already be available to you.

Security awareness training can be successful even with a small budget. Hopefully the tips you've learned here and the case studies will help inspire you.

2. KNOW YOUR REQUIREMENTS

If you are in the financial industry, payment card issuers and banks have specific security controls that must be included in security awareness training. The same holds true for healthcare providers. Any organization that is considered a covered entity or business associate must follow HIPAA standards for privacy and security compliance. Check with your People team and legal counsel to determine what compliance regulations are in scope and make sure you include those when you plan your program. Check your company's policies to see what training requirements you have.

If your organization develops software, your technology team will need to have additional training in secure coding techniques.

If your organization is subjected to audits, you may need to track participation in your training program and be able to report who has completed training.

3. GATHER YOUR CONTENT

Once you know your budget and training requirements, start gathering the content of what your program will include. Start with the training team within your People team. They typicially have a learning platform and that platform may have security awareness topics you can use. Work with your technology teams to verify that they have access to, and are completing, training in defensive coding and network security.

Subscribe to newsletters to stay informed of data breaches and cyber-safety techniques. Use these materials to plan supplemental training, bulletins or your own company newsletter. It's important to weave security awareness content into the daily work life of your organization.

4. PLAN YOUR PROGRAM

Don't let security awareness training be relegated to one boring annual training session with lots of slides and a quiz at the end. Guaranteed that if you do this, your teams will do the bare minimum to pass.

Tie security awareness training to your company culture. If you have a company intranet, or billboard, use those to post quick security awareness reminders and change them out at least a couple times a year.

Be creative and use friends and colleagues to generate ideas that go above and beyond the standard, boring training. You've got the ability to transform your program - do it!

5. LAUNCH

Now that you are confident that your training contains the required learning, and you've planned your first campaign, it's time to launch. Schedule your first training session or event with a small group of trusted advocates. You'll gain more confidence as your program grows and matures.

Don't worry about being perfect - be human. Let people see your passion for the training content and your concern for their cyber security.

Start small, but just start!

CHAPTER 4

Successful case studies you can learn from

SureIT

Dental Practice

Treat your Password like your Toothbrush

Most people don't realize that dentists and dental practices are considered healthcare covered entities and therefore must adhere to HIPAA Compliance regulations.

We built a customized security awareness program that included weekly newsletters, monthly training , a dedicated Slack channel and fun ways to correlate good oral hygiene to good cyber hygiene.

This training campaign spanned 6 weeks, with a new graphic and new way to safeguard your password. This is password management training that is fun and effective. We incorporated the images that dentists and hygienists could relate to, highlighting key security awareness tactics. These memes were posted in the newsletter, Slack channel and company intranet at various times throughout the campaign.

In addition to this weekly training campaign, the security awareness program highlighted news articles about ransomware threats that were realized in similar medical and dental practices, insider threat reporting processes, and HIPAA compliance standards.

Face Time

Train your team to reach out for help

Hackers are using emails, text messages and even phone calls to sway innocent victims to act quickly. We included this slide into a security awareness presentation and on the company intranet to encourage people to recognize when something is unexpected.

If they find they are making these faces, team members are encouraged to stop, think, do some research or reach out to a trusted Information Security professional (like an IT Help Desk) for assistance.

This is a fun and non-judgemental way to let training participants know that hackers are targeting them continually. We are all human, and need to work together to combat fraud and hacking.

This slide also highlights that if you find you have clicked the link, please contact someone who can mitigate the risk.

SUREIT.WORKS

Want to go deeper?

Work with me one-on-one

I host security awareness training sessions disguised as tea parties or ice cream socials. I can tailor an effective and informative security awareness training program for you.

SCHEDULE TIME FOR A CONSULTATION