CLICK ARMOR™
Click With Confidence

SECURITY AWARENESS INDUSTRY REPORT

OUR CHALLENGES & SOLUTIONS TO THE BIGGEST TRENDS IN CYBER SECURITY

Q1 2023

PREPARED BY

SCOTT WRIGHT

Welcome to our Q1 2023 Security Awareness Report. We've combined all our knowledge on the biggest trending topics from the quarter into one file. In this report, you'll find challenges, identified by renowned industry professionals, and solutions created by our team here at Click Armor.

Our challenges were identified in our Q1 Cyber Security Awareness Forum that we host twice every month. The guests of these panels are industry leaders, coming from organizations like the Global CTI Group and Central Security. The guests range from newly joined students in the industry to high-level CSOs. These guests are surveyed to produce the stats included throughout the report.

Follow us on LinkedIn to catch the next CSAF.

Password Managers

A major topic of discussion this quarter was password managers, specifically LastPass, after the breach it endured in Q4 of 2022. Although this might have scared many people away from using tools like password managers, it's still a great cyber security hygiene practice to encourage your users to utilize.

It's good to remember that no password manager will be perfectly safe. They are constantly targeted by attackers (robbers rob banks because that's where the money is, attackers attack password managers because that's where the passwords are). This is why it's important to do your research and still have good password practices even if you use a password manager platform.

These breaches might make you want to ditch password managers altogether, but chances are your employees will then resort to even more dangerous password practices like having easy-to-guess and repeating passwords.

25% of poll participants don't use a password manager.

Industry Leader-Defined

Challenges

UNSAFE PASSWORD PRACTICES BY EMPLOYEES

"One of the common password managers I see is Microsoft Excel or Word or even a notepad. I did an assessment and for one individual I was able to hack into her account. She was a part of the accounting department and I found an Excel Sheet with all of her login information including some banking information."

-Tom Bigos, Central Security

UNCERTAINTY AROUND THE TRUSTWORTHINESS OF ONLINE PASSWORD MANAGER

"I can understand the hesitation of wanting to keep your passwords online. After LastPass, we found out it wasn't as secure as we were led to believe. Then you have to wonder if all the other password managers are the same."

-Jim Guckin, Customer Bank

BREACH MANAGEMENT

"The most popular password managers are going to get attacked. So, you have to be able to say "Ok, we're fine. Let's move past this.", but you have to ask, "When is it enough to move?."

-Jim Guckin, Customer Bank

Click Armor

Solutions

1. Do your research.
Figure out which password manager makes the most sense for you or your organization. If you are uncomfortable with an online password manager, there are options for offline password managers, too. A good password manager will have transparency in their password protection and past breaches and requirements for your passwords and master password.

2. Educate your staff on good password practice.
Host a session going over password best practices or spread the message from the top down.

3. If your passwords are breached, take action.
After a breach, always assume your accounts are in danger unless stated otherwise. Change your master password and all your other passwords.

Want to learn more?

Download our latest guide for Advanced Security Awareness Tips and Tricks for Security Managers from Q2 2022.

DOWNLOAD

Password Checklist

- ☑ *Longer than 12 characters*
- ☑ *Include at least one symbol*
- ☑ *Includes lower/uppercase*
- ☑ *20+ character master PW*
- ☑ *MFA turned on*

Cyber Insurance

Cyber insurance includes a lot more than our specialty, security awareness. It can include general IT requirements and rules for your organization to follow. It's important to remember that cyber insurance isn't a magic wand that makes all your cyber security training needs disappear.

It's a remediation tool or a backup plan. Not your primary source of security. You have to consider the possibility of having to pay for ransom, having your brand reputation damaged, having to wait years for payouts, and losing important data, cyber insurance will not stop these things from happening. That's why you cannot depend solely on it as your cyber security program.

However, it's still a great backup plan. It could save your business when the worst happens. The average security breach in the US costs a business over 4 million dollars. So, unless you are ready to pay that (or more) unexpectedly out of pocket, signing your business up for cyber insurance should be at the top of your list.

63% of poll participants don't have cyber insurance at their company.

Industry Leader-Defined

Challenges

RAPIDLY RISING PREMIUMS

"A lot of my clients have reported that they are having a hard time getting their policies renewed without extreme increases in their premiums."

-Anthony Leece, Syntax Security Solutions Inc.

LOSING POLICY RENEWALS

"I've heard certain situations where the insurance company did not renew a policy because a company didn't have a,b,c. I even had one client where their insurance company didn't renew their policy because they said last year we asked you to do a, b, c and you didn't."

-Tom Bigos, Central Security

GROWING LIST OF REQUIREMENTS

"Every year with any organization, the bar for their cyber insurance gets higher and higher. Especially when it comes to awareness training. The most breaches come from a phishing email, it seems to be the main way in, so awareness training requirements are going to keep becoming stricter."

-Jim Guckin, Customer Bank

Click Armor

Solutions

1. Invest in a quality awareness program.
As breaches become more common in all organizations, awareness programs are going to become a more popular requirement for insurance companies.

2. Answer your questionnaire questions truthfully.
It's better to be truthful and have higher premiums than lie about the training you have. If you have a breach and require a payout, they will probably do an inspection. You don't want to give them a reason not to pay you.

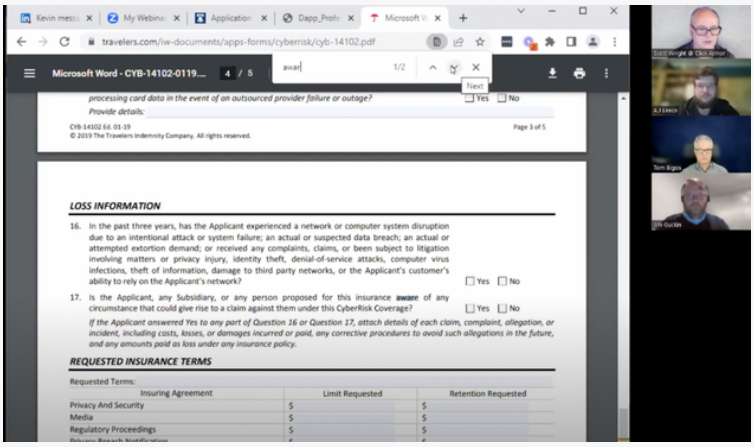
3. Do more than the minimum.
Always try and be one step ahead of your cyber insurance. Even if certain training isn't a requirement yet, implement it now so that when the time comes that they do require it, you're not scrambling to put something together or miss out on a better premium.

Is your program quality?

Learn how to quickly assess and train your employees with our Phishing Assessment Optimizer.

DOWNLOAD

Watch our panel on cyber insurance & review real insurance applications with us.

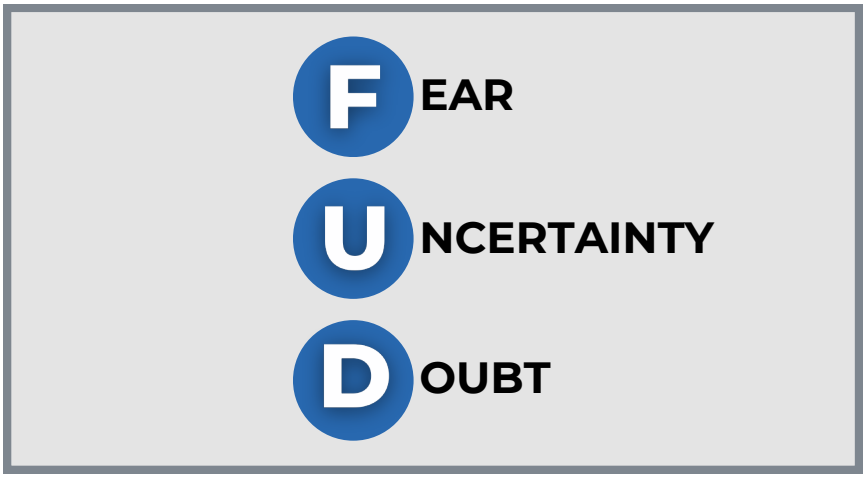


Industry Statistics

Statistics can be a great tool to discover the population's awareness of certain security problems and compare it to what action we want them to take. They can also be a great tool to gain a new client, by making them aware of the future that could await them.

But, sometimes they can be used in the wrong way and create FUD. This can lead to the opposite of our goal and instead scare people so much that they don't even want to bother with security awareness at all.

In this section, we'll talk about the right way to use statistics from organizations like the Canadian Internet Registration Authority (CIRA) and how to use your own statistics for better storytelling.



Industry Leader-Defined

Challenges

DATA ISN'T TRULY RELEVANT

"People like to use what I would call "fake math" for scare tactics. Like, I don't know your susceptibility rate, the size of your organization, or how you're being catergorized. Most of these platforms tend to put you in a conglomerate that may or may not fit the demographic of your workforce."

-Fletus Poston, CrashPlan

SMALL SAMPLE SIZES

"There's no requirement to be statistically significant. You hear numbers that are for a whole industry, but even if the sample size is a thousand, they could be representing tens of thousands or even millions of companies."

-Tyler Sweaney, Global CTI Group

STATS SCARE AND THEN DISCOURAGE

"I've seen statistics presented in a way that is just disheartening. It gets to the point to where the business thinks, "Well, if that many people are going to click on the link, then what's the point? I'm just going to get cyber insurance and call it a day."

-Tyler Sweaney, Global CTI Group

Click Armor

Solutions

1. Get your own stats.
Do your own research and use benchmarking to businesses that you know are similar to yours.

2. Look at the before and afters of your business.
If you don't have access to statistics from other businesses, you can use the before and after statistics from your own business to prove that something does or doesn't work.

3. Give solutions with hope.
There are scary risks in the security world, and that's just the truth. So, if you do decide to share a "scary" statistic, ensure that you also share a hopeful solution to help alleviate the FUD.

4. Use stories to elaborate on your statistics.
Use general statistics for an initial presentation or an initial call You never know if you are talking to a creative mind or a mathematical mind, so use a story to elaborate on your statistic. This will help your potential client relate more to the story and understand the need for security.

Need your own stats?

Request a free team phishing assessment now, and schedule one for after you implement your program.

REQUEST A DEMO

89%

of poll participants believe statistics should be less than 2 years old to be "relevant".

Oversharing & OPSEC

The National Institute of Standards and Technology (NIST) defines operations security as, “a systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities.”

In a more casual way, operational security is protecting your organization against accidental or unnecessary release of information by employees which could make it easier to launch successful attacks on sensitive information or systems.

With the newly popularized innovations of things like screen sharing and controversial apps like TikTok, our companies are at risk for accidental exposure now more than ever.

88% of poll participants believe employees overshare & make attackers jobs easier

Industry Leader-Defined

Challenges

OVERSHARING BY EMPLOYEES

“Oversharing has become a natural thing that we, as a society, are conditioned to do. We live on social media and we’re conditioned to put everything out there like an open book. And a lot of the times your username is easily traceable back to your name at your organization.”

-Ryan Healey-Ogden, Click Armor

BALANCING MARKETING & SAFETY

“You have marketing advisors saying left right and center that if you’re not on TikTok then your business is going to fail. But, it’s a platform that is in the news a lot for being a risk to fundamental security. So, it’s that drive between hitting your goals for the year and keeping your people safe."

-Ryan Healey-Ogden, Click Armor

IDENTIFYING SENSITIVE MATERIALS

“The five steps of operations security is a flow. So, if you don’t even do the first step of identifying your sensitive materials, everything flows from there. From my perspective it either comes from a place of ignorance or lack of awareness.”

-Tyler Sweaney, Global CTI Group

Industry Leader-Defined

Challenges

NOT ENOUGH REGULATION

"There just isn't enough governance regulation to prevent the misuse of data information. Even though you are signing privacy agreements when you use someone's software, it doesn't give them permission to pass it on."

-James Castle, Cyber Security Global Alliance

VALUING CONVENIENCE OVER SAFETY

"If people don't know that convenience is a double-edged sword then they become even more reliant on that convenience. You have to show them what information they are exposing and prove that convenience isn't a necessity, but it's human nature to want to take the easier path."

-Ryan Healey-Ogden, Click Armor

NEW OPPORTUNITIES FOR EXPOSURE

"One thing people have overlooked that the pandemic did is the open source intelligence you can get from screen-sharing. How many meeting have we been in that someone shares something and it's the wrong tab or the entire screen?"

-Ryan Healey-Ogden, Click Armor

Click Armor

Solutions

1. Be aware of your privacy environment.
You have to be aware of the privacy commitments you and your employees are making when you sign up for an application. For example, if you are a paid GSuite member, they don't index your data, but if you are a free customer they are. Read through privacy agreements to make informed decisions.

2. Arm your employees with the best knowledge.
Keep your employees armed with engaging and useful training. The more your employees know, the less likely they are to make mistakes.

3. Get support from the top down.
Top executives are typically the first ones to disable MFA or password changing policies. Have conversations and present them with statistics that will get them on board to support your training and policies.

4. Have locked-down devices for your employees.
Have devices that are used for company reasons only. This will help them separate personal and business security and be more diligent with their work phone.

Our favourite OPSEC resources:

- *PrivacyGuides.org*
- *CIS Security Guides*
- *Click Armor Mini Course*

Artificial Intelligence

Obviously, artificial intelligence has been making headlines all year, but how does it relate to security awareness? It can make our jobs easier yet harder. It can make your training better, but yet require it to be more difficult.

The most important point is that it's not too early to take action. Although it's hard to predict what the future exactly brings for artificial intelligence, it's important that we still act quickly in order to protect our employees and our businesses.

Don't be afraid of these emerging technologies, and instead embrace them and learn how you can use them to your advantage and how you can prevent them from becoming a disadvantage.

43% of poll participants think attackers will benefit more from AI than security companies.

Industry Leader-Defined

Challenges

IMPROVING PHISHING EMAILS

“AI could make phishing emails a lot more realistic and it is quite terrifying actually how realistic they are, because all the things we tell people to look out for, like spelling mistakes and bad grammar, they're not really in those emails anymore.”

-Michelle L, Channel 4

CONCERNS AROUND JOB SECURITY

“We already have a shortage of critical talent in cybersecurity and now we're seeing AI discouraging people from potentially going down this road because they're like, well, the computer's going to do it for me, and what am I going to do to be able to compete against that?”

-Ryan Healey-Ogden, Click Armor

DWINDLING TRUST

: One of the scary things for me is the advancement of things like deep fakes using A.I. My concern is that we're going to stop trusting what we see on any media because it can be faked so easily. It's always going to be a cat and mouse game.

-Scott Wright, Click Armor

Click Armor

Solutions

1. Teach your employees about tone.
Consider adding tone to your cyber security awareness program. Help your employees learn how to use critical thinking to identify if the tone matches the sender since incorrect grammar and spelling are becoming less and less common.

2. Use AI to your advantage.
AI can still benefit your security awareness training if you use it properly and safely. Some professionals use it to help them reword cybersecurity slang into easily digestible dialogue for their employees.

3. Create company-wide AI regulations.
Remind all of your employees that any internal company documents or information should ever be put in Chat GPT or any type of AI. Consider creating a form or open Q&A session where employees can confirm what is and isn't allowed.

Watch our panel discussion on artificial intelligence to hear our predictions for the future.

Contact Us

We hope you found good value in this Click Armor Q1 Industry Report. If you need help implementing any of our recommend solutions or have questions about the identified challenges please connect with us with one of the options below. Stay safe!

Contact Us

Book a Call Here

info@clickarmor.ca