BEAUCERON
SECURITY

2021 ANTI-PHISHING TRAINING

DOES ANTI-PHISHING TRAINING WORK?

Over the past twenty years, security awareness programs have been designed with the intent to share knowledge of key cybersecurity concepts.

In today's world, with a new data breach or major hack in the headlines every week, people are more aware than ever before that cybersecurity is a problem that requires attention. The problem for security awareness professionals has shifted from building awareness that security matters to changing long-held individual behaviours and organizational security culture. With 85% of malicious breaches still coming from the human elements of cybersecurity [1], it is evident that while people may know about cybersecurity, they are still engaging in risky behaviours.

A great example remains the continuing problem of phishing, social engineering attacks that use e-mail as the delivery method.

While people often know what a phishing attack is, they struggle to handle phishing attacks in practice. When we compound this with the fact that the volume of phishing attacks doubled in 2020 [2], the need for changing these behaviours in handling technology is greater than ever before.

Do anti-phishing education programs work?

A common concern raised by some cybersecurity professionals is whether organizations should conduct phishing simulations as part of their education and behaviour change programs. Many of the arguments for not doing these activities are based on the programs not achieving a 0% click rate. Some of the arguments have to do with the emotional consequences of poorly executed phishing simulations which can alienate or anger organizational team members.

As we will demonstrate with our findings, anti-phishing programs are an effective and essential part of every organization's cybersecurity effort. The aim of these programs is not to get to zero, but to create compelling learning opportunities with a chance to learn from experience or easily demonstrate adequate knowledge of what phishing is as well as motivate to do the right thing about it, specifically to report phishing threats to the organization.

We'll also demonstrate ways organizations can minimize negative employee sentiment by using clear, and pro-active communications combined with a clear and fair approach to education and phishing.

Anti-phishing programs are an effective and essential part of every organization's cybersecurity effort.

Summary of Findings

Do We Still Need Anti-phishing Programs?

According to the Internet Crime Report published by the FBI, the most common type of cybercrime in 2020 was phishing [3], yet anti-phishing training programs are too often deprioritized by organizations.

To demonstrate the value of a well-designed anti-phishing training program, we have analyzed a data set of 4.3 million phishing simulations sent to over 350,000 users across 325 organizations. Using the Beauceron platform, organizations have been able to see fast and continued improvements in their cybersecurity cultures:

OVER 90 DAYS
- **85% decrease in clicks**
- **99% increase in reports**
- **11% decrease in ignores**

OVER 2 YEARS
- **90% decrease in clicks**
- **285% increase in reports**
- **37% decrease in ignores**

Our Effectiveness

Click Rate

The click rate is the most common metric referred to in security awareness campaigns. This rate indicates how many employees are interacting with phishes. When training has not occurred and users are blind-phished, click rates hover around 30%. It has been proven that educating employees decreases the likelihood of clicking on phishes [4].

Organizations should, therefore, strive to create a knowledgeable employee base, which would reflect in a click rate below 5%.

While the click rate should be low, the goal of the anti-phishing training should not be to drive the click rate to 0%.

In the real world, attackers use innovative strategies to infiltrate organizations, such as exploiting hot topic issues, targeting users, and creating random and short-lived campaigns. As such, a 0% click rate may indicate that the phishing simulations do not accurately reflect the types of attacks someone would receive in the real world.

BEAUCERON SECURITY

The goal of anti-phishing training should not be to drive the click rate to 0%.

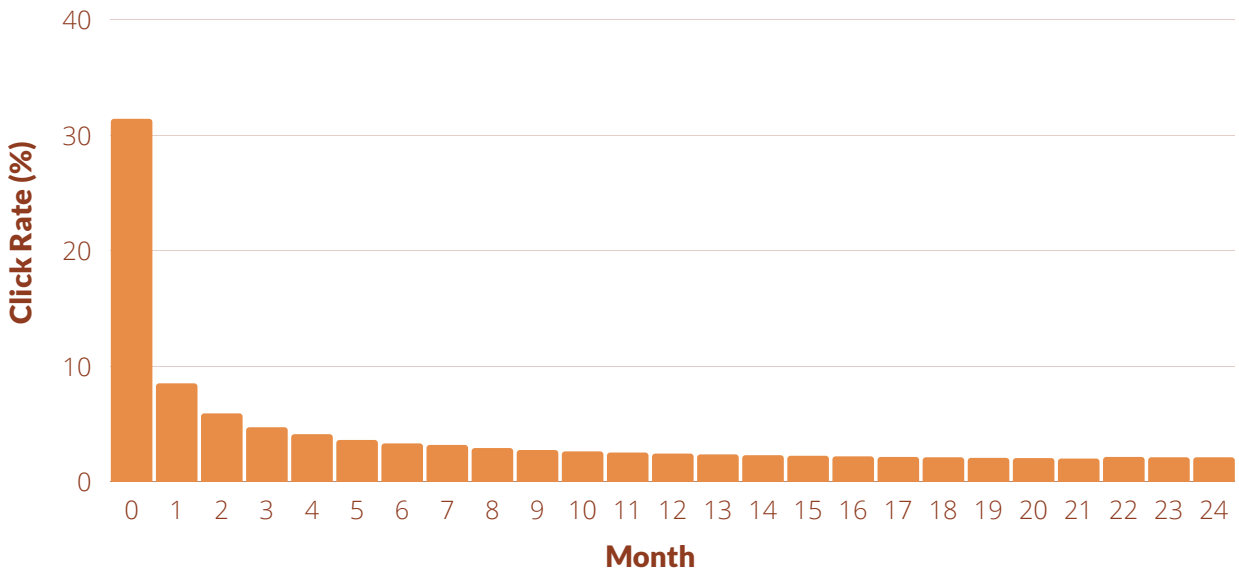
To achieve a representative click rate for your organization, consider the following:

- Randomize templates to control for content and phish difficulty.
- Randomize when phishes are sent to control for external events, e.g., time of day, discussion between employees.
- Send phishing simulations on a frequent basis. We would recommend monthly phishing to control for external events and to provide users with continuous training.
- Send up-to-date phishing simulations. Phishing trends change regularly, so to make your employees as resilient as possible, train them with simulations that mimic phishes out in the wild.

Using the Beauceron platform, administrators can leverage the automation capabilities to determine a representative click rate. The following results demonstrate the fast and sustained results organizations can achieve:

Leverage the automation capabilities in the Beauceron Platform to see fast and sustainable results.

Immediately after training:	**8.5% (73% decrease)**
After 90 days:	**4.7% (85% decrease)**
After two years:	**2.1% (90% decrease)**



*Month 0 is based on an industry average blind phishing rate between 30-40%.

BEAUCERON SECURITY

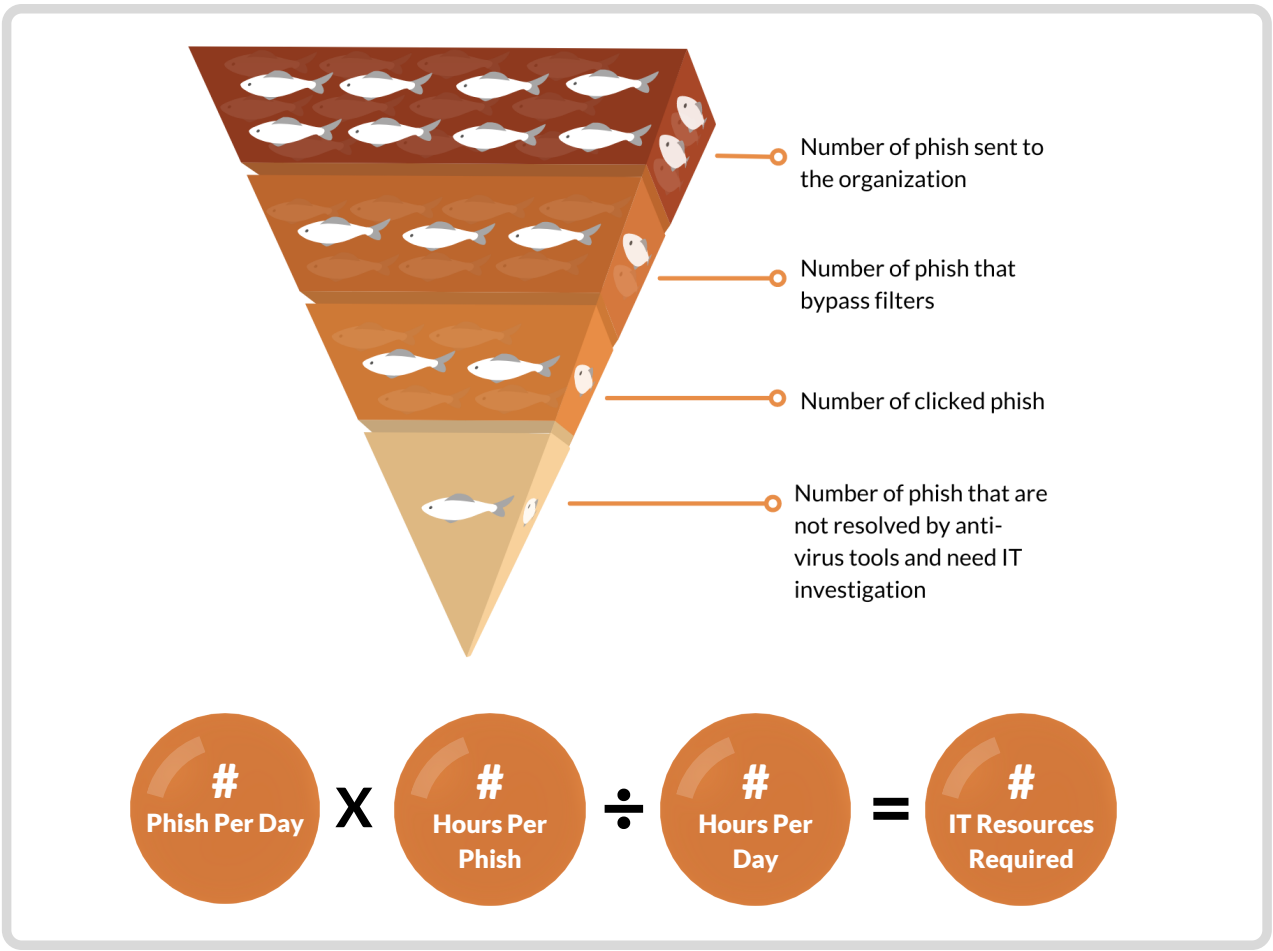
Did You Know: Over 15% of phishing clicks occur between 8 AM and 9 AM?

Leveraging the Click Rate to Measure Return on Investment

An organization's target click rate can be determined based on its capacity to handle incidents, taking factors such as the number of daily malicious emails and the effectiveness of technological solutions into account.

Having a target provides IT a direction, but this click rate does not take any proactive measures into account. Changing employee's attitude and behaviour allows IT to get ahead of possible threats while building a stronger, more caring line of defense.

In calculating an organization's capacity, you can leverage key metrics from your anti-phishing program:



BEAUCERON SECURITY

Phishing metrics can help organizations better understand their phish capacity.

IT & Employee Relationship

When someone clicks on a phish, they can experience emotions such as frustration, embarrassment, or fear. Starting a cybersecurity program on a negative note can discourage employees and hinder the development of the supportive learning environment people need to change and adopt new behaviours. Instead of taking the chance that employees feel "tricked" by IT, we recommend that the platform administrators:

- Inform employees of the new program
- Train users
- Communicate to users that they will receive simulations
- Set expectations on the number and frequency of simulations they will receive

These actions allow IT and employees to start building an open, transparent relationship that will allow for the necessary cybersecurity growth.

Blind phishing is performed by some organizations so that they can determine a control click rate. This click rate serves as the baseline, from which stakeholders can evaluate the effectiveness of training.

While we understand that some organizations desire to blind phish their users, we generally recommend against blind phishing for a better IT & employee relationship.

Click Rate Isn't the Only Metric That Matters

The click rate has traditionally been used to evaluate the benefit of cybersecurity awareness platforms, where the blind phishing rate marks the baseline click rate from which users should improve after training. Several studies [4] have shown that the click rate should decrease after employees are educated. As such, the need to validate that click rate decreases through training has reduced. We instead recommend that users receive training from day one so that organizations can focus on building a resilient employee base.

Value from the platform can still be determined through a decreasing click rate, yet administrators should also look for the platform to encourage an increased report rate and a decreased ignore rate. These measures indicate the adoption of cyber secure behaviours and attitudes and allow IT teams to be proactive about potential threats.

Did You Know?
77% of users who click on a phish do so within 24 hours of it arriving in their inbox.

The click rate is only one key metric that organizations should consider.

Report Rate

The report rate and the time to report phishes are key metrics to measure employee behaviour and the cybersecurity culture. Organizations should strive for a high report rate and a quick time to report. These rates indicate that employees are knowledgeable, but that they are also engaged and care to play a positive role in the organization.

Reporting phishes quickly allows IT teams to be proactive about potential threats. When a phish is reported, IT teams can investigate the phish and determine if it is malicious. These emails also allow IT to understand the types of emails that are bypassing their technological solutions. Based on the trends that are evident from the reported phishes, IT can update the filters to reduce the number of emails that are undetected.

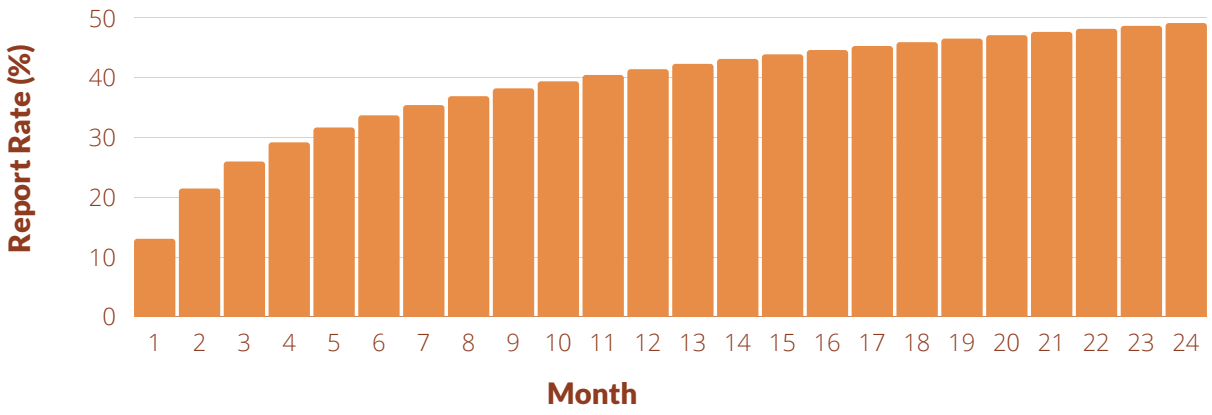
IT is also able to quickly act if a phish is reported after it has been clicked. Any one can click on the right phish at the right time, so encouraging employees to report the phish even if they have clicked it gives IT valuable time to determine the impact of the click.

To build a proactive cybersecurity culture:

- Find a solution that makes reporting suspicious emails easy, like a "Report a Phish" button.
- Adopt solutions that help detect threats in the reported emails. Phishing websites and spam are on the rise, so use solutions that can maximize the IT team's time.
- Communicate the importance of a cybersecure attitude and measure the ignore rate to identify users who may need to be re-engaged.

As evidenced by a 285% improvement in report rates, organizations have had great success building a positive cybersecurity culture.

Immediately after training:	**13.0%**	
After 90 days:	**25.8%**	**(99% improvement)**
After two years:	**49.1%**	**(285% improvement)**



BEAUCERON SECURITY

A proactive cybersecurity culture helps increase report rates up to 285%.

Ignore Rate

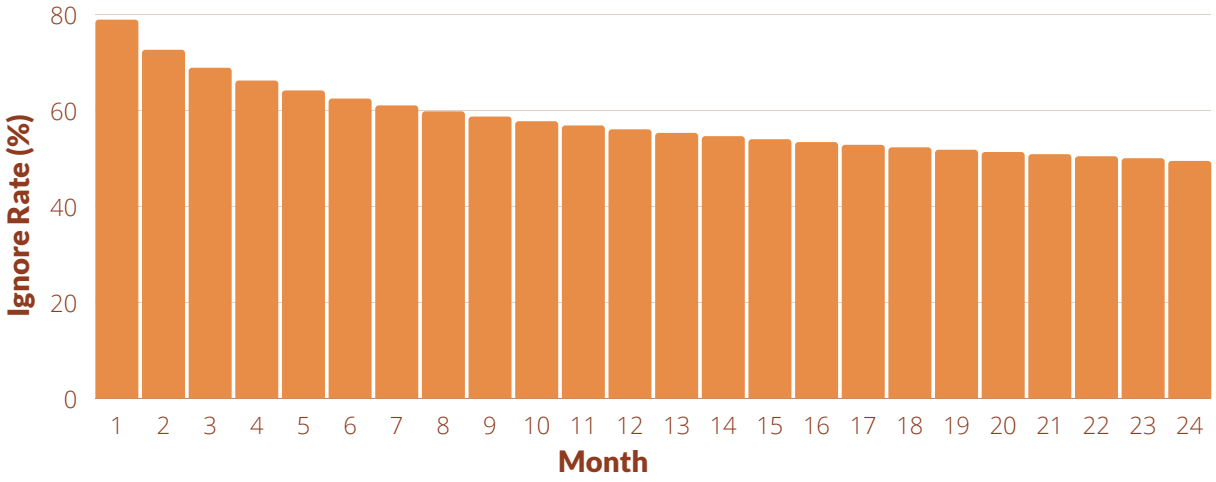
When phishes are not clicked or reported, they are being ignored. Ignoring phishing simulations is an important metric to measure as it indicates that employees may require further education to better recognize phishes or that they may be disengaged.

As you educate your employees on phishes, here are some factors to consider:

- Engage with employees with tools such as surveys to understand if they know what a phish looks like and how to report a phish.
- Schedule recurring training to occur at least once every 5 months. Research has shown that this interval is best practice even with an optimistic view on knowledge retention [4]. This regular training interval would allow employees to learn about emerging phishing trends as well. Changes in the phishing landscape can be communicated in the training material, with examples of threats that targeted the organization. Real attacks can also be copied with the malicious links removed to leverage as phishing simulations to directly improve employee resiliency.
- When delivering training, aim to contextualize the information. Explaining the "why" to employees helps them to understand the important role they play in the line of defense, which can change their attitude toward cybersecurity and thus increase the effectiveness of the training [5].

Using the Beauceron platform, users can decrease their ignoring behaviour by 37%.

Immediately after training:	**78.8%**
After 90 days:	**70.0% (11% decrease)**
After two years:	**49.5% (37% decrease)**



BEAUCERON SECURITY

Decreasing the ignore rate by 37% indicates increased awareness & education levels.

If the employees have not yet adopted a cybersecure attitude:

1) Help the employee understand how they play an important role in the line of defense

Explain how reporting phishes allows your organization to investigate potential threats more quickly and the positive effect this plays in the organization.

Provide employees with cybersecurity tips that they can use both in the workplace and at home, so that they understand the relevance of cybersecurity training.

2) Publicize the organizational & leadership buy-in

Show the engagement from leaders and encourage leaders to regularly discuss the importance of cybersecurity with employees.

3) Provide feedback

Celebrate users as they engage with the cybersecurity program. This celebration could be a thank you message to users who reported all their automated phishes, a shout-out to users who were engaged in a cybersecurity conversation, or a gift card to the user that has the lowest risk score.

4) Make it a safe space

Communicate that any individual may click on a phish if it is the right phish at the right time. While it is important to decrease the number of clicked phishes, it is even more important to report the phish after it has been clicked. This can enable people in the organization to feel comfortable admitting a mistake has been made so the IT team can investigate it even quicker.

Our Approach

At Beauceron Security, our mission is to change the conversation about awareness and towards empowering people to feel in control of the technology they use and rely on every day. Beauceron's cloud-based platform enables organizations and individuals to change risky cyber behaviours. The platform engages users, encourages learning, and helps them to recognize their role in cybersecurity. It helps organizations create and sustain positive security cultures.

Beauceron's market-leading automation enables security professionals to spend their time on what matters most, engaging with employees and driving their strategic security program goals forward.

Features

Here are some key features that will help you make your cybersecurity program a success:

Personal Dashboard

To drive behaviour change, each user has a personal risk score in the platform. This score is broken down by their awareness, exposures, incidents, and rewards. As users exhibit positive behaviours, such as reporting phishing simulations with the Report a Phish button, their risk score decreases. Not only are these positive behaviours celebrated through their personal risk score, but also through badges and a friendly leaderboard.

Education

The number one thing we hear in the field is that vast amounts of standardized content is not as valuable as custom relevant content. It can be difficult to gain buy in from employees if they can't connect with the material.

Beauceron includes a library of bilingual content that can be automatically assigned to individuals or groups either proactively or reactively after an incident. Courses can also be made available for self-enrollment.

Enabling employees to self-enroll in security courses is both a great way to provide education that is relevant for an employee's home life (social media, etc.) and proactively identify candidates across the organization that may have an interest and skill in cybersecurity.

Behaviour Reinforcement

The security team can leverage Beauceron to assign rewards and incidents and attach remedial training if desired. This enables the security team to reinforce positive behaviour and follow up with the employee to explain how to avoid an incident in the future.

Phishes

Simulations

Our platform helps organizations move beyond phishing campaign click rates with deeper insights to which employees regularly know how to spot and report cyber risks.

Beauceron provides a variety of automated phishing simulations that can easily be customized to meet the organization's needs. Organizations can configure automated, random simulations to run on a biweekly, monthly, or quarterly basis as well as manually schedule specific campaigns, or run campaigns without supplemental training. With Beauceron's in-tool editor, organizations can easily customize or create their own phishing simulations.

Once implemented, consider phishing simulations and remedial training on autopilot.
Simulations are integrated into the individual risk score. Once a simulation is reported, employees are automatically rewarded for the positive security behaviours.

Detecting Real Threats

To reduce the workload of your security team, organizations can leverage the Beauceron Analyst as a PhishForward Add-on Service. The Analyst draws in threat data from several external sources and scores emails based on the email metadata – including identifying or recognizing potentially malicious senders, malicious links, or attachments. The Analyst will decide whether the email is likely malicious or not. Configurable thresholds for scoring allow you to customize the sensitivity of the Analyst.

Conclusion

At Beauceron, we've demonstrated that anti-phishing programs that are fully integrated into a positive behaviour change platform are an effective way to reduce risk and engage employees.

Our platform can power world-class security awareness and behaviour change programs that will deliver better and faster results for your organization.

Positively Change Behaviour

At **Beauceron Security**, our mission is to change the conversation about cyber risk, empowering people to feel in control of their technology.

We've created a powerful software-as-a-service platform to help organizations tackle cyber risk. Our comprehensive platform drives security programs that change behaviour. We engage users, encourage learning, and help them to recognize their role in cybersecurity.

Beauceron's high degree of automation can save the organization thousands of hours while arming leaders with real-time performance metrics to quickly illustrate compliance.

Founded in 2016 by security professionals, Beauceron Security serves organizations in every major industry vertical with clients ranging from 10 employees to 100,000+ employees.

Let's Get Started

Simplify your user onboarding, pull real-time compliance reports, and create custom relevant content in a fraction of the time.

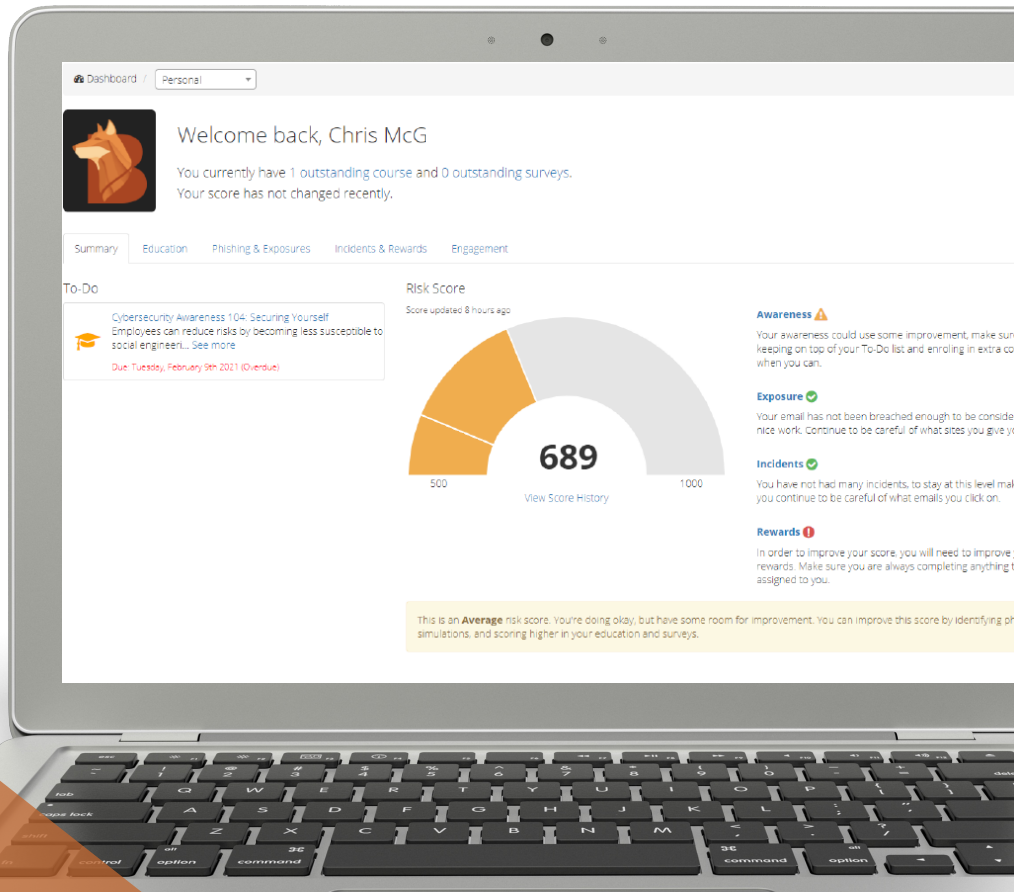
Your time is valuable, put it where it matters most – engaging your community.

Our customer success team is ready to help you achieve these results.

Contact Us

Office: 1 (877) 516-9245

sales@beauceronsecurity.com



BEAUCERON SECURITY

References

[1] Verizon, "2021 Data Breach Investigations Report," 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed 2021].

[2] APWG, "Phishing Activity Trends Report," 2021. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf. [Accessed 2021].

[3] FBI, "2020 Internet Crime Report," 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Accessed 2021].

[4] D. Jampen, G. Gur, T. Sutter and B. Tellenbach, "Don't click: towards an effective anti phishing training. A comparative literature review," Human-centric Computing and Information Sciences, vol. 10, no. 1, pp. 1-41, 2020.

[5] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Computers & Security, vol. 42, pp. 165-176, 2014.