HOXHUNT

Buyer's guide to phishing training

Ebook - August 2020

Table of contents

01

Executive summary

Cyber crime is on the rise globally and phishing emails and websites are not going away anytime soon. Even sophisticated security programs whose infrastructure protections and technical filters block out close to 99% of malicious content are not enough today. Cyber criminals are increasingly exploiting on the 1% of emails that get through to employees and focusing their attack vectors on people with spear phishing and social engineering tactics.

IBM's researchers reported in the Data Breach Report for 2019 that the average total cost of a data breach worldwide in 2019 was 3.92 Million USD (but it's almost double that in the US at 8.19 Million USD). That is a large sum of money, which is why organizations need to do whatever it takes to avoid a data breach, as the high cost of work associated with it, and the potential impact on your reputation could be detrimental to operations.

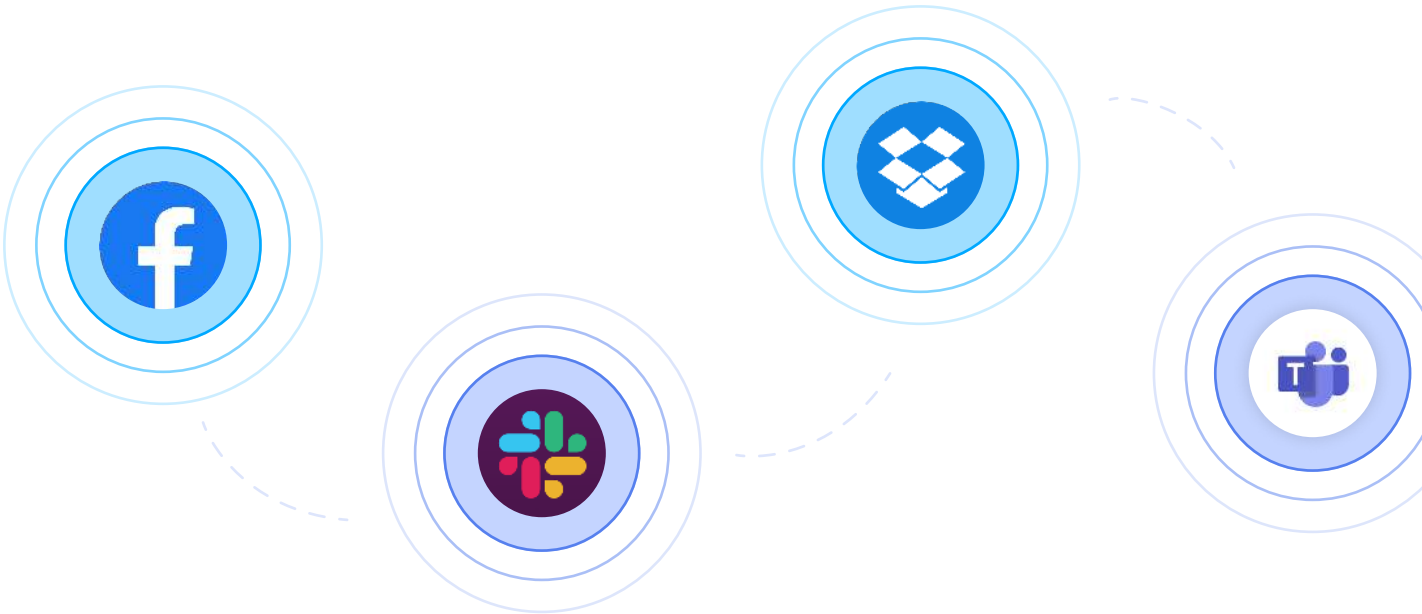
Many organizations have a siloed approach to security, which results in a lack of accountability across the organization, and a sense that security is only an IT problem, according to Accenture's study. This is why training employees to think and act differently with security at the forefront of their minds throughout their workday is vital. Keeping the organization secure should be a team effort.

There are a lot of different approaches to security awareness training, and a slew of vendors offering a range of services. This guide was created for decision-makers looking for a new phishing training solution that focuses on reducing the human IT risk in their organization. In this guide, we will cover some of the main reasons why phishing training is not always effective within the organization. We will also highlight the main criteria you should consider when making your decision about which modern phishing training solution meets your organization´s needs and positively impacts and lowers your risk profile.

Did you know?

Attackers don’t only use email for delivering attacks. They are exploiting popular social media sites, instant messaging applications, and file-sharing services.

Facebook, Slack, Microsoft Teams, Dropbox, and other popular platforms could serve as the initial point of penetration into the enterprise.



Source: Security Boulevard

02

Criteria to look for in a modern phishing training

Major factors of differentiation in phishing training can be linked to the following criteria: user experience, personalization, reporting metrics, behavior change, and automation.

These criteria can help you assess your options in buying a human-first phishing training that can help you reduce risk in your organization.

User Experience

Employees don't like doing tasks that interrupt their normal workflow for a significant period of time. Training is usually mandatory, but you can incorporate training into an employee's regular workflow without stopping productivity for hours at a time. People have trouble focusing on content that is longer than 5-7 minutes, and you want to be respectful of your employee's time and utilize it efficiently to maximize learning.

Small teachable moments to show learners how to improve in the future based on their past behavior can be an effective method to train and communicate to employees about security awareness topics.

💡 **Tips to Improve the Employee Experience:**

- Short training moments
- Encourage user interaction for active learning
- Implement training that can be embedded in an employee's workflow (email client, work phone, laptop, etc.)
- Reward success for positive reinforcement
- Try different approaches
- Monitor user feedback (NPS rating of different vendors and qualitative feedback)

Gamification is one example of how you can make training personalized and more enjoyable for the user. When assessing different vendors, consider the user experience carefully. Your employees are going to be the ones using the training on a daily basis, and you want it to be relevant, minimally disruptive to their work, and easy to use

Personalization

If employees don't feel like the training is relevant to them, then they will lose interest fast. This is why you should compare a vendor's level of personalization applied in their phishing training, in terms of employee's cyber knowledge (IQ), role, department, and language of training content.

Not every employee has the same level of cyber knowledge, and everyone has a different background when it comes to cybersecurity. This is why phishing training can't be administered in the same way to everyone.

📌 Personalized Learning Paths

Personalized learning paths are a factor to consider in your vendor search for a training solution. If an employee keeps failing simulations, you might need to take a step back and send out easier attacks for the employee to spot. Once the employee sees that he or she can be successful, the employee will become more engaged, and you can start sending attacks that are more difficult. If employees continuously fail, they will feel defeated and lose momentum and interest in the training. Positivity is the key to engaging people and keeping them coming back for more!

🇫🇮 Language of Content

Another important level of personalization is the language of the security training content. Make sure to ask prospective vendors whether their training solution covers the local languages of your employees. In case the vendor does not provide the language(s) that you need, you should always ask them whether they are planning to add it in the future.

Reporting Metrics

Many organizations and vendors track the click rates of phishing simulations, but this metric needs to be considered carefully. An organization may be using very simple simulations or very difficult challenges, skewing results to one side of the bell curve or the other. If everyone received the simulation at the same time, it is likely some employees working in an open office setting will also give their coworkers a hint not to click on the fake campaign.

This can lead to a false sense of security if your training is too easily spotted. Passing a few tests per year does not show your organization is prepared how to respond to sophisticated modern attacks.

📊 Reporting Rates and Failure Rates

Two of the main KPIs in phishing training are reporting rates and failure rates. When employees are engaged in training, reporting rates of simulations will increase. Most likely the reporting rates of real threats will increase as well. This will give security teams increased visibility into the attacks the company is receiving and allow them to react faster.

Failure rates of different vector types can also highlight areas where employees may need additional training in the future, and the progression and decline of failure rates can show the success of training over time.

Scammers are after your passwords, financial information, identity, and money.

Source: Stanford University

Behavior change

One of the main pillars of behavior change is reinforcement, and continuous reinforcement and repetition will transform your behavior into a habit. In security awareness training, the behavior change that the employer wants is to teach employees how to react appropriately every time they receive potentially malicious content. The other objective is for employees to understand why reporting threats is important to the organization.

👍 Positive Reinforcement

Research has proven that workplaces need to consciously overcome a habit of trying to scare people into action and highlight when employees do the right thing or reach their goal with a reward or positive feedback. **When employees report a phishing simulation correctly, and then they are given positive feedback, they will be more likely to report real phishing threats that hit their inbox in the future**. This is the whole point of phishing training.

💻 Frequent and Continuous Training

Another key component to behavior change is the frequency of training. When choosing a vendor, keep an eye out for the quantity of phishing simulations promised per employee on an annual basis. Continuous, on-going training will keep your employees on their toes, and repetitive actions drive a lasting behavioral change.

Together, positive reinforcement and frequent training are key traits that improve employee satisfaction with security awareness training. They also help shift the perception of cybersecurity to a more positive topic in the organization that everyone participates in.

Automation to enable security teams

Automation is a key driver in productivity improvements and cost savings. This is why you should consider the impact automation could make on your security team in regard to phishing training.

The level of automation can also play a large part in how personalized you can make your training content, as sending out 36-48 personalized emails per employee each year can add up to a lot of work hours.

👀 Why is automation in phishing training important?

Many organizations develop phishing campaigns for their employees manually, which can be very costly and time consuming. Organizations that develop their own training from start to finish may look at vendor options to help with some components of the process or the whole thing.

When choosing a new partner for phishing training, you don't have to replace all of your existing security awareness efforts. It might make sense to use phishing training in addition to some of the other initiatives you have planned throughout the year. The two main benefits from automation in phishing training is the automation of delivering personalized, relevant, and frequent training, plus the automation of threat identification, classification, and escalation.

Attackers are using Zombie Phish and Shortened URLs. It's more difficult to identify a shortened link as malicious.

Source: Comparitech

Automation to enable security teams

⏳ Time savings

Some training solutions offer a library of content (videos, phishing templates, etc.) that can be categorized and personalized in more detail with some manual work, and security teams get access to the content to pick and choose what they want to send out to each department. Although this gives the security team hands-on control over each simulation, it also requires a lot of extra planning work. Phishing simulations can also be sent out automatically with some vendors.

The level of automation in a phishing training can also be relevant when it comes to content. If security teams spend significant time internally researching the latest attacks to develop relevant content for their employees, the organization may be losing out on valuable resources of their security team members. Having a vendor that regularly updates their content to include the latest attack variations and themes can be a big-time saver for your security team.

According to IBM, the average time to identify a breach was 206 days in 2019.

Source: IBM

INTERESTING FACT

A Google researcher reported that 45% of internet users don't know what phishing is. Make sure your employees don't belong to the 45%!

Source: Security Boulevard

03

How to research your vendors?

When searching for any security vendor, it is important to do some research, not only on the vendor’s website, but also to read up on thoughts from peers and community members.

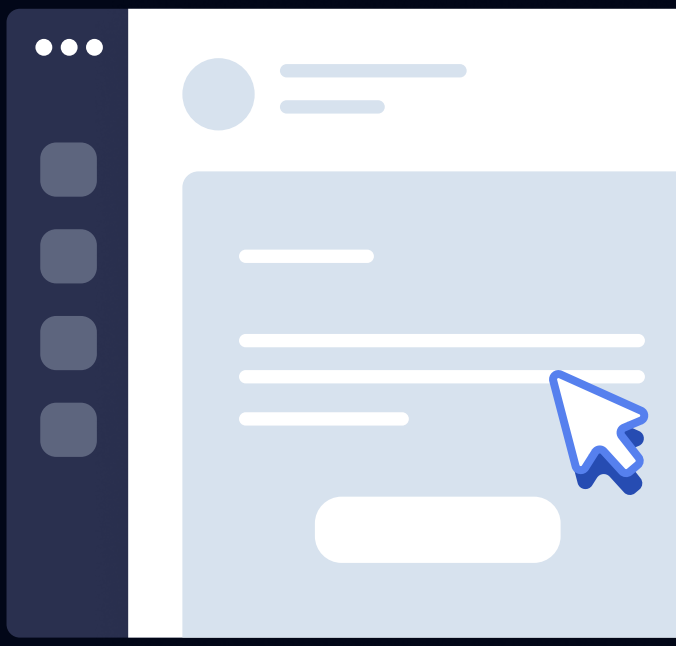
We suggest review websites such as G2, which shows unbiased reviews on user satisfaction with different products and software. We also suggest that you take a look at trending vendors in the industry and compare what they are doing differently.

Learn more

DID YOU KNOW?

Phishing attacks are highly sophisticated, targeted, and short-lived. It's cheap and simple to create the exact replica of a Microsoft 365 login page and launch a phishing campaign.

Do you think it's easy to recognize these attacks? See our video how difficult it is to recognize a well-crafted Outlook 365 phishing campaign.



Source: Security Boulevard and Hoxhunt

04

Questions to ask prospective vendors:

Before you meet with potential vendors, it’s good to create a list of questions that matter for you.

It will help you compare vendors upon the same criteria and have all the answers you need to make a decision.

We gathered the most frequently asked questions to help you brainstorm.

Questions to ask prospective vendors

User experience

1. How do you encourage employees to participate in the training?
2. How much time does the training take out of an employee's regular work week?

Personalization

3. What language options do you have for delivering training content and support?
4. What happens when an employee fails a phishing simulation once or multiple times?
5. Does everyone receive the same training at the same time or is training personalized in any way to employees?
6. How often is the training content updated? Is content updated in each language regularly?

Reporting Metrics

7. What type of progression can you expect to see after 1 month of training, 6 months, and 1 year (reporting rates, participation rates, etc.)?
8. What KPIs do you measure? What are the reporting capabilities?

Behavior Change

9. How frequent do you send simulations per year to each employee or how frequent do you recommend (for solutions that offer templates)?

Questions to ask prospective vendors

Automation

10. About how many manual hours would be required from our security team to send out a campaign for X number of employees? (100, 10,000 or 20,000)
11. Where does malicious content (phish emails) go once it has been reported by an employee?

Implementation of Training and Technical Capabilities

12. What are the steps of the onboarding process?
13. Do I receive any help with communication before the roll out of the new phishing training?
14. Do you have threat reporting tools?
15. Can the training be integrated with other tools? e.g. Microsoft ATP?
16. Does it work on all devices? Which devices? Which email clients?
17. How does the pricing work? Do you pay for each element of training separately or is it a cost per employee?

Good to remember

No business is too small to get caught up in phishing!

Scammers increasingly target small businesses, especially that more and more employees work remotely.

Source: Verizon

05

About Hoxhunt

Hoxhunt empowers your employees to shield your organization with a human-first approach to phishing training. We do this with an automated cyber training program that transforms the way your employees react and respond to the growing amount of phishing emails.

To get to know us better visit our About page.

06

Sources

Cyber-crime during the COVID-19 Pandemic.

http://www.unicri.us/news/article/covid19_cyber_crime

Cost of a Data Breach Report

https://www.ibm.com/security/data-breach https://www.ibm.com/downloads/cas/ZBZLY7KL

The Cost of Cybercrime

https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Reinforcement and Behavioral Change

https://opentextbc.ca/organizationalbehavioropenstax/chapter/reinforcement-and-behavioral-change/

What Motivates Employees More: Rewards or Punishments?

https://hbr.org/2017/09/what-motivates-employees-more-rewards-or-punishments

G2: Best Security Awareness Training Software

https://www.g2.com/categories/security-awareness-training

List Of Security Awareness Training Companies To Watch In 2020

https://cybersecurityventures.com/security-awareness-training-companies/

Tale of the Tape: Top 5 Reasons Phishing Attacks Haven't Dried Up

https://securityboulevard.com/2020/07/tale-of-the-tape-top-5-reasons-phishing-attacks-havent-dried-up/

2019 Data Breach Invesgtigation Report.

https://enterprise.verizon.com/en-gb/resources/reports/dbir/

Internet Security Threat Report 2019.

https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Phishing statistics and facts for 2019–2020

https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

What's New in the 2019 Cost of a Data Breach Report

https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

HOXHUNT

Interested in getting to know Hoxhunt more?

Click here for a demo of our platform on our website.

If you have a question feel free to contact marketing@hoxhunt.com.