RAPID7

HOW TO PHISH YOUR BUSINESS (AND GET MANAGEMENT'S BUY-IN)

Answering key questions about the value, cost, risk, and execution of a phishing awareness program

TABLE OF CONTENTS

INTRODUCTION: WHAT MANAGEMENT WANTS TO KNOW

You know that phishing and related social engineering techniques targeting users are linked to more successful data breaches than any other form of cyberattack, making them today's number one attack vector.

You know that it is impossible to prevent phishing attempts by purely technical means.

You know that a phishing awareness program can dramatically reduce the success rates of phishing attempts.

But the members of your management team probably don't know much about what a phishing awareness program is, or why it's important. They may have an exaggerated idea of the risks, and because they are bombarded by proposals for new projects, they want to make sure they pick ones that will provide material benefits to the business.

So, how do you get management's backing for a phishing awareness program?

First, you frame the program in the right way—as an educational campaign that will help employees protect themselves and your company.

Second, you answer key questions such as:

- Why is a phishing awareness program important?
- Will it be expensive?
- What are the risks?
- How do you plan to execute the program?

This guide is packed with advice on how to frame your proposal for a phishing awareness program, how to answer likely questions, and how to show that your initiative is one of the best investments your company can make in cybersecurity.

SEEKING MANAGEMENT APPROVAL

First things first: Do you really need management's approval for a phishing awareness program? Typically you wouldn't ask non-technical executives to bless the use of a next-generation firewall or a SIEM (except as a line item in the budget).

But a phishing awareness program is different. It touches most employees in the organization. It takes people away from their work, for a few minutes at least. It leads to discussions around the coffee machine, and it might raise concerns about privacy.

If these discussions bubble up to senior managers, you don't want them to be surprised. In fact, you want those managers to be on board with the campaign and ready to explain why phishing awareness is important to everyone in the company.

> "You don't want senior managers to be surprised. You want them to be on board and ready to explain why phishing awareness is important to everyone in the company.

WHO TO APPROACH, AND HOW

Which senior managers do you approach, and how do you make your case? The answer depends on the culture of your company. The expected practice may be to submit a written proposal, schedule a meeting and present slides, or just sit down for an informal discussion.

But keep in mind:

- You want to reach executives with enough clout to convince other senior managers to allow their people to participate.
- No matter the presentation medium, you must prepare answers to the most likely questions about value, cost, risk, and execution, because these questions are certain to come up.

Framing the Initiative

A phishing awareness program **is not** a piece of technology or a new toy for the IT and security staff (although there is a technology component).

A phishing awareness program **is not** a technique to manipulate people or play "gotcha" with negligent employees (although it will let them know when they have been careless).

A phishing awareness program **is** an educational campaign that shows employees how to protect themselves and the company from cybercriminals.

It is important to keep this perspective not only when presenting the proposal to management, but also when planning and executing the program. Despite what skeptics may think, phishing awareness is about empowering people to make better decisions, and you should design your process to produce that result.

Showing That Phishing Is a Serious Threat

To grab the attention of senior managers, start by describing the problem you want to solve. In the case of phishing, statistics and anecdotes can help you make your case.

For example, you can point out that according to a Verizon study:

- Phishing was involved in over 90% of security incidents and breaches that involved social actions (that is, attacks based on human mistakes).
- Ninety-five percent of the phishing attacks that led to a breach were followed by some form of software installation; many also caused people to disclose confidential information.[1]

[1] Verizon 2017 Data Breach Investigations Report (DBIR): Attack the Humans! section.

Other helpful data points may include:

How prevalent is phishing?

- One industry organization finds over 87,000 unique phishing campaigns every month, launched from around 50,000 websites.[2]
- Phishing and social engineering attacks are the number one concern of security professionals, and are their most time time-consuming activity on a daily basis.[3]

Do phishing attacks affect many enterprises?

- Phishing was seen in 72% of organizations surveyed in 2017, more than any other type of threat.[4]

How many people fall for phishing emails?

- Different surveys and tests have found anywhere from 7% to 45% of users clicking on a link or opening an attachment in a phishing email. Even 7% ensures that attackers can find many potential victims in any organization.

How much damage is done by phishing campaigns?

- The FBI estimates that business email compromise (BEC) scams alone (which are based on spearphishing emails that appear to come from company executives and other insiders) caused $5.3 billion in losses to businesses worldwide in 40,000 incidents over three years.[5]

How many phishing emails hit your company in a month?

- Symantec found that in 2016 slightly more than one in 2,596 emails was a phishing email.[6] So you can take the number of emails that enter your network in a month, divide by 2,596, and come up with a reasonable estimate.

The idea here is not to deluge your management with statistics, but to show that there are hard numbers proving that phishing is a very serious threat.

> “Phishing and social engineering attacks are the number one concern of security professionals, and are their most time time-consuming activity on a daily basis.

[2] APWG Phishing Activity Trends Report, 1st Half 2017

[3] 2017 Black Hat Attendee Survey

[4] SANS Institute: 2017 Threat Landscape Survey.

[5] FBI: Business E-Mail Compromise - E-Mail Account Compromise, the 5 Billion Dollar Scam

[6] Symantec: Internet Security Threat Report, Volume 22

DESCRIBING A PHISHING AWARENESS PROGRAM AND HOW IT HELPS

Most managers will have only a hazy idea of what a phishing awareness program entails. Give them a concise overview that they will be able to remember and repeat.

As mentioned earlier, it is important to frame the phishing awareness program as a campaign to raise the awareness of phishing threats and motivate employees to help block them.

> One study found that training reduced clicks on phishing emails between 26% and 99%, with an average improvement of 64%.

A typical program includes four elements:

- **Training,** which educates employees on why phishing is harmful and how to detect and report phishing attempts.
- **Phishing simulations,** which test whether people apply the training under real-world conditions and reinforce the lessons when they don't.
- **Real-time reporting of phishing attempts,** which makes it easy for employees to do the right thing and help IT detect real phishing attempts.
- **Follow-up training** for employees who fell for the phishing simulations, which helps them improve their response.

There is evidence that phishing programs have an effect on improving employee behavior. One study found that training reduced clicks on phishing emails between 26% and 99%, with an average improvement of 64%. That doesn't solve the entire problem, but it represents a substantial improvement.[7]

While the value of preventing employees from falling for phishing emails is clearly important, the value of improving reporting should not be overlooked. If 20 employees fall victim to a phishing attempt before someone reports the incident, the cybercriminal has 20 opportunities to plant malware before the security staff can respond. If the first employee to receive the phishing email reports it, however, then the attacker may have no chance.

[7] Ponemon Institute: The Cost of Phishing & Value of Employee Training

Explaining the Cost

Phishing awareness programs don't cost very much when compared with the benefits.

Direct costs are quite low, and the subscription costs for powerful phishing simulation management tools are typically modest as well. Unless your organization is very large, the effort required to create and run the simulations amounts to only a few hours per week.

Training will require time from the instructors who are preparing and delivering the information. However, that effort can be limited by using written documents or media like teleconferencing and video. If you decide that classroom training will be most effective, it can be included in sessions that provide other types of IT or human resources training.

Phishing awareness training will obviously take employees away from their work for short periods. But this can be weighed against the costs of not providing such training. Different studies have evaluated the combined cost of dealing with a single successful phishing attack as $3.8 million for a typical company. That includes the cost of dealing with malware, productivity losses, and business disruption.[8]

Minimizing Risk

Most managers are sensitive to risk, for the good reason that they have seen plenty of initiatives that produced unintended consequences. They are likely to be concerned that a phishing awareness program might create resentment if it creates a feeling that employees are being spied on or manipulated.

But you can reassure them that you have anticipated this concern and will minimize the risk by following a few guidelines.

First, create a core phishing education team that includes at least one executive or high-level manager, someone from human resources or corporate communications, and a few individuals representative of the employee population, as well as the IT analyst or administrator who will be conducting the simulations. Having broad representation in this steering committee ensures that you will take into account diverse viewpoints, including those of employees and managers. It also creates a network of champions for the initiative within the organization.

> "A phishing education team with broad representation ensures that you will take into account diverse viewpoints and create a network of champions.

Convey repeatedly to employees that the program will never be used to embarrass or punish individuals or departments. The simulations are designed as learning tools that will help employees get better at detecting and reporting suspicious emails, so they can better protect themselves and the company.

Finally, put in place safeguards to protect privacy. For example, the simulated attacks should never retain sensitive information such as passwords and social security numbers. Anonymity should be preserved wherever possible, and published results should never single out individuals.

[8] Ibid.

WHAT TO INCLUDE IN EMPLOYEE TRAINING

If you are asked, be ready to give an outline of the proposed training. Typically that would include:

- The dangers of phishing to individuals and the company (conveyed by the statistics and examples you have already gathered for management).
- How to detect suspect emails by identifying Indicators of Phishing (IOP), such as: odd or unknown senders, unexpected attachments, misspellings and bad grammar in the text, links that don't match the address spelled out on the page, and phrases frequently used in scams.
- How to report suspected phishing emails, ideally through a button in the email client or browser.
- The plan to use phishing simulations as a learning tool, and the safeguards in place to make sure that privacy is preserved.

The methods of delivering this education depend on the company, but they might include a document, an online video, company or department meetings, classroom training, or some combination of these. These might be publicized through "all hands" emails, employee newsletters, corporate intranets, social media, or all of the above.

RUNNING THE PHISHING SIMULATIONS

Simulations involve creating email campaigns that closely replicate the real-world phishing attacks most likely to be used against your specific organization. These are created with phishing simulation tools, employed by an IT analyst, administrator, or member of the security operations team.

The typical process is to:

1. Research the types of phishing attacks most likely to be launched against the company (mass phishing), or specific departments or individuals within it (spearphishing and whaling).
2. Use a phishing simulation tool to create emails, attachments, and web landing pages that reflect an attacker mindset. These can be customized to match the versions most likely to target the company, and even individual departments or roles within the company.
3. Use the tool to create a "training page" for each simulation, explaining to unwary employees what happened, how it could have affected them and the company, and what to do in the future.
4. Select a target group for the simulation.
5. Send the email to the target group and monitor the results.

Because the purpose of the exercise is to improve employee behavior, it is important to spend time building out the training page, making it as robust and educational as possible..

Most organizations will also offer follow-up training to employees who fall for phishing attempts in the simulations, to reinforce the original training and to offer extra information on how to avoid the particular mistakes made.

> "The simulation tool can customize realistic emails, attachments, and web landing pages to match the versions most likely to target the company and departments within the company.

SUMMARIZING THE BENEFITS OF A PHISHING AWARENESS PROGRAM

At some point somebody might say something like, “This training and simulation are very nice, but how do they actually produce results?”

Part of the answer is that they significantly reduce how often people click on links or open attachments in phishing emails. As mentioned earlier, one study found that training reduced clicks on phishing emails between 26% and 99%, with an average improvement of 64%.

But you should also highlight two other important benefits.

First, the simulation tool should be able to collect statistics on the success rate of attacks, including details such as what percentage of employees open phishing emails, click on a link, go to a compromised website, click on an attachment, and report emails that contain Indicators of Phishing (IOP). These statistics provide critical insights for the IT group and management in terms of weak points, risks, and the progress of the phishing awareness program in reducing dangerous employee actions.

Second, improving the speed and accuracy of reporting suspect emails can provide a huge benefit to the organization. As discussed earlier, if the first employee to receive a phishing email reports it, IT security can respond before any damage is done.

In fact, to improve the rate of reporting, the organization should:

- Make reporting as easy as possible through a phishing hotline, email address, or even better, a button in the email client or browser.
- Emphasize reporting repeatedly during training, including why it is critical to report suspicious emails immediately, and how to do it.
- Adjust incident response processes to make maximum use of phishing reports as confirmation when phishing attacks are occurring and to alert the IT organization.

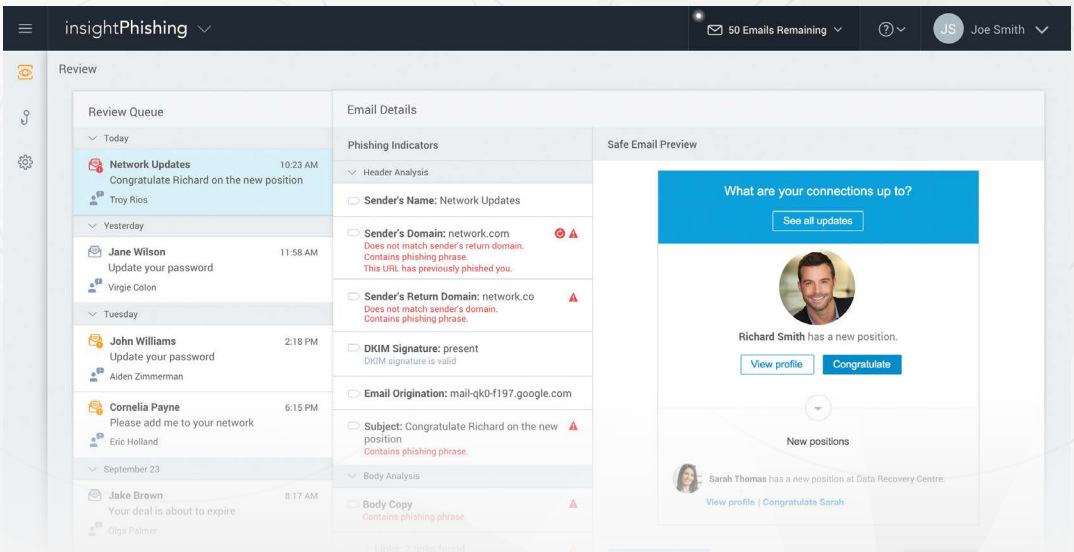
> “Improving the speed and accuracy of reporting suspect emails can provide a huge benefit to the organization.

FINDING A GREAT TOOL FOR PHISHING REPORTING AND SIMULATIONS

Okay, we're slipping in a short commercial here. InsightPhishing from Rapid7 is an easy-to-use tool for creating and managing phishing simulations and reporting suspected phishing attempts. It addresses the needs of managers, employees, and the IT administrators or analysts who will be running the simulations and using the reports of suspected phishing attempts. InsightPhishing:

- Is easy to learn and use
- Gives you pre-designed templates that mirror real-world attacks based on an attacker mindset
- Makes it easy to customize those templates for your industry, company, and departments
- Helps you create effective training pages
- Makes reporting suspect emails easy through a button in the email client or browser
- Evaluates messages to determine if they contain Indicators of Phishing (IOP), enabling analysts to identify active phishing campaigns more quickly.
- Provides statistics on simulation results and employee reporting, so analysts can track the improvement of the organization's phishing awareness over time
- Never collects confidential information
- Is very economical
- Was designed by Rapid7, a leading provider of vulnerability management, penetration testing, application security, incident detection and response, and log management solutions, including the world-renowned Metasploit penetration testing software

Learn more about how Rapid7 InsightPhishing can protect you against phishing attempts at: rapid7.com/insightphishing



ABOUT RAPID7

Rapid7 (NASDAQ:RPD) powers the practice of SecOps by delivering shared visibility, analytics, and automation so that security, IT, and Development teams can work together more effectively. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for more than 7,200 organizations across more than 120 countries, including 54% of the Fortune 100. To learn more about Rapid7 or join our threat research, visit www.rapid7.com.