CLICK ARMOR™
Changing cybersecurity behavior

Expert Guide

Addressing Employee Vulnerability to Phishing Risks

BY SCOTT WRIGHT

Certified Information Systems Auditor

Click Armor Corp.
August, 2021

Introduction

While over 90% of security breaches start with phishing email messages, according to security vendor Trend Micro, many organizations don't realize how hard it can be for employees to recognize a phishing attack. And if employees can't recognize a suspicious message when they are faced with one, the chances are high that they will become a victim if they are targeted.

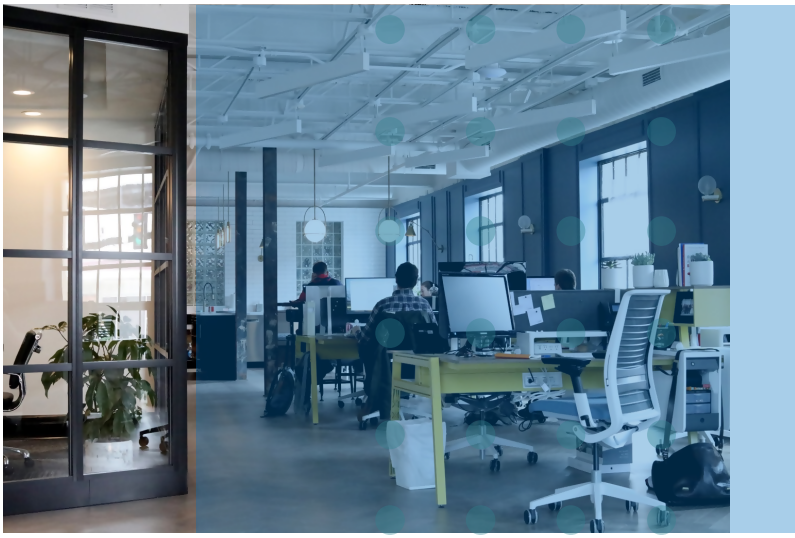
Even organizations that have the best security safeguards in place can still experience breaches, especially if they are targeted by cyber attackers who do a bit of research about the organization and its employees.

Finding employees who have administrative rights, or access to valuable information, is not that hard. And it only takes one email recipient with the right conditions to cause a disaster such as "ransomware" that can bring your operations to a halt.

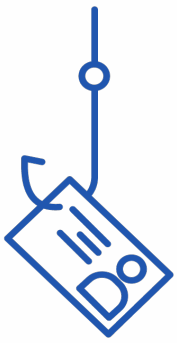
Overview

This paper highlights the ways that attackers influence employees to take dangerous actions, and what employers can do to improve employees' ability to spot and avoid these risks.

This is where so-called "spear-phishing" email techniques are used. When an attacker has identified a single employee, or a group of employees that may have access that can get the attacker closer to their ultimate target, they begin looking for plausible situations to which these employees will likely respond.



Then, they will create an email message that is likely to cause the recipient to click on a link or attachment. This may be all the attacker needs to launch a new variant of undetectable malware on the recipient's computer, or to lure them to a "spoofed website", where sensitive information can be gathered, such as login passwords. So, the key aim for the attacker is to get the recipient to click on that link or attachment.



There is almost always a pretext situation that can get an employee to click.

The situations used by attackers in phishing email messages to convince recipients to take action are called "**pretexts**". They are simply "made-up situations", but are designed to be plausible, based on the knowledge an attacker has about the target recipient. But if people don't feel that they are likely to be a target, they often don't recognize one of these situations as being an attack.

In general, attackers that use phishing emails try to ***exploit employees' emotional triggers***. There are almost an unlimited number of pretexts that can be used to elicit an emotional reaction from an employee, especially if the attacker knows even a small amount of information about that employee or the organization.

Below is a list of the **10 of the most common emotions** used by attackers in phishing messages. Employees often don't recognize one of these situations as being an attack.

Greed or desire to obtain more of something

Messages might offer something for free, or at a price that is too good to be true, like hotel stays.

Ambition

Messages might have enticing hints of exclusive career opportunities.

Laziness

Messages might offer tools or tips that promise to simplify tasks.

Fear of financial loss

Messages might deliver a warning of a financial penalty if action is not taken by an imminent deadline

Curiosity

Messages might have an unusual or uncommon subject and content, which promises an interesting outcome if the action is taken.

Desire to help

Messages might play on a recipient's sense of generosity and helpfulness, with a plausible situation that requires assistance.

Fear of disciplinary action

Messages might appear to be from a person of authority, with a request that implies consequences if the request is not actioned.

Fear of embarrassing information exposure

Messages might contain a claim that an attacker has obtained sensitive personal information that the recipient is not likely to want exposed.

Impatience

Messages might create a situation for which an employee feels they are being asked to do some unreasonable task by management, with an option for them to take a recommended alternative action to avoid the task. (i.e. "Do the following steps to complete the process, or click here to ask for an exception.")

Security

Attackers will even send messages that prey on employees' desire to improve security, by informing them that there has been some kind of incident for which they must take immediate action to prevent further damage.

There are many more emotions upon which spear-phishing pretexts can be created by attackers. But the point of highlighting this short list of 10 emotional triggers is to illustrate the wide range of possible scenarios that an attacker may use to target individuals in phishing attacks.

Telling employees to "***be careful of suspicious messages***" is not usually sufficient to prepare them for some of these carefully pretexted situations.

How employers can reduce employee vulnerability to phishing messages

Clearly, there is a need to educate employees about how tricky some spear-phishing email messages can be, with the aim of reducing their vulnerability to these kinds of attacks. And there are many online training programs that do a good job of explaining the problem and how to reduce the risk of being tricked. However, many training programs are only able to address the "employee understanding" of risks and policy guidance. As a result, these programs are not really addressing some of the key issues that make employees vulnerable, beyond just understanding.

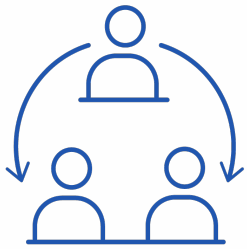
In fact, while traditional programs may improve employee awareness and understanding of cybersecurity risks, they are not really arming the employees with techniques to actually change their behavior to reduce their vulnerability.

There are a number of reasons why traditional training, alone, may not result in employees making the correct choices when they are facing these kinds of attacks.

Here are the main challenges and some potential solutions for improving employees' resistance to spear-phishing attacks:

Employees see security as "the IT security team's job”

When employees do not see an alignment between their interests and what the organization is asking them to do, they often feel it is not important. If they don't see an impact from clicking on suspicious links, employees won't change their behavior. For example, employees may not realize that the average cost of a data breach for a small to medium-sized business is over $2 Million, and that the vast majority of breaches involve employee vulnerability or negligence.



Tip #1: Align employees’ interests with the organization’s need for them to recognize and resist attacks. Organizations need to create an environment where it is easy for employees to recognize how their decisions impact not only the business, but their own situation. Compensation bonuses or other rewards based on employee proficiency and behavior in making decisions that management sees as important can align their interests more effectively with the organization.

Policies that “*a dead person can comply with most of the time*" are not very memorable

Policies that give employees negative instructions such as, “Do not click on suspicious links…” or “Avoid…” or “Never…” not prescriptive. It can also be hard for employees to remember "negative guidance", even when they are at a logical decision point, and when they have the time to consider taking the safe path.

Tip #2: Give employees practice at rare risk situations.

Organizations need to help employees in making the right choices to comply with policies. One of the most effective ways to do this is to give employees experience with making those decisions in a safe environment, where there are not real consequences, but where employees can get the right positive or negative feedback on their choices.

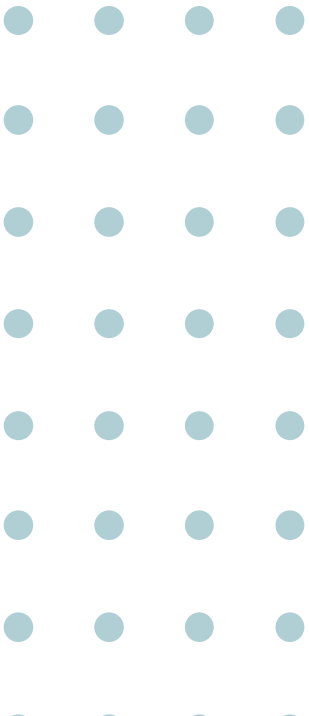
Employees want to focus on completing their tasks; they don't want to interrupt their work routine at random times.

It is natural for us to want to complete the task we are working on. So, it is hard for employees to recognize when situations arise that require them to stop what they are doing to take extra precautions. Analyzing the component patterns within a phishing email message, such as the sender, the links and the content, is not something that employees will naturally want to do, even if they know the policy guidance.

Tip #3: Focus on pattern recognition. Organizations need to focus on helping employees recognize **when** they need to interrupt a task based on a recognized risky situation, to address any potential dangers that might be at play. Then they can make the right decision, and get back to their main job tasks.

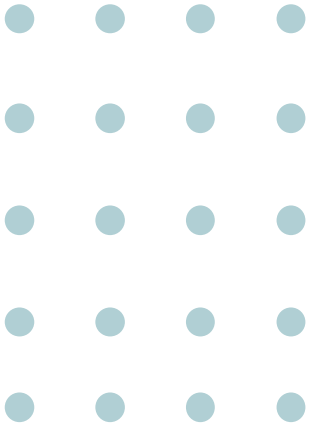
In many cases, addressing the above objectives isn't easy because it may not be possible to expose employees to specific threat environments or decision points on the job in a way that would allow you to measure their choices. However, **it is possible to use games, exercises and simulations** to engage employees in a focused way, and to exercise and assess the decisions they may see only rarely on the job.

.



If employees are engaged and assessed in this way, with proper feedback that doesn't "demotivate them", then they will be better able to recognize these situations, and will be more likely to make the right decision.

By ***adding gamification elements*** to the highest risk areas of your security awareness program, you can add a new dimension that not only improves decision-making of employees, but also shows employees that you are serious about changing behavior to protect your business information and processes.



At Click Armor, we help businesses avoid costly ransomware and fraud incidents through gamified learning that engages employees, to build a self-defending team.

http://www.clickarmor.ca

If you would like to learn more about how gamification and game-based learning can change employee behavior, and measure proficiency in difficult areas, please contact us for a demonstration of the Click Armor Arcade for Cybersecurity.

You can contact us by phone at 613-693-0997

Or, you can meet with a consultant now at www.clickarmor.ca/contact

About Scott Wright

Scott Wright BASc, MBA, is CEO and founder of Click Armor, and is a veteran cybersecurity coach and consultant. He has over 20 years of experience in IT Security, and has taught security awareness to business teams for over 10 years. In addition to creating Click Armor, Scott has co-hosted The Shared Security Podcast since 2009, and created the Symantec Honey Stick Project for assessing risks related to human vulnerabilities.