ADVANTIO
an Integrity360 company
your security in mind

LEARN MORE
ADVANTIO.COM/PHISHING-CAMPAIGNS

Phishing Campaigns

According to the Verizon 2022 Data Breach Investigations Report, “the human element continues to drive breaches.” In 2022, more than 82% of breaches involved the human element.

Humans are consistently considered the weakest link in security and the path of least resistance for an attacker to breach an organization’s defenses. As businesses continue to deploy anti-phishing strategies and educate their users about cyber security, cybercriminals continue to improve phishing attacks and develop new scams.

A Phishing attack is an email scam designed to steal personal information from victim organizations. Cybercriminals use phishing to obtain sensitive information by disguising as a trustworthy organization or reputable person in an email communication. Phishing is popular with cybercriminals because it enables them to steal sensitive financial and personal information without having to break through the security defenses of a computer or network. A form of social engineering, phishing tricks users into giving away information and/or access by clicking links, opening attachments or sharing credentials.

These attacks can be low-tech and highly targeted making them highly effective and lucrative for attackers. They’re not only set up to

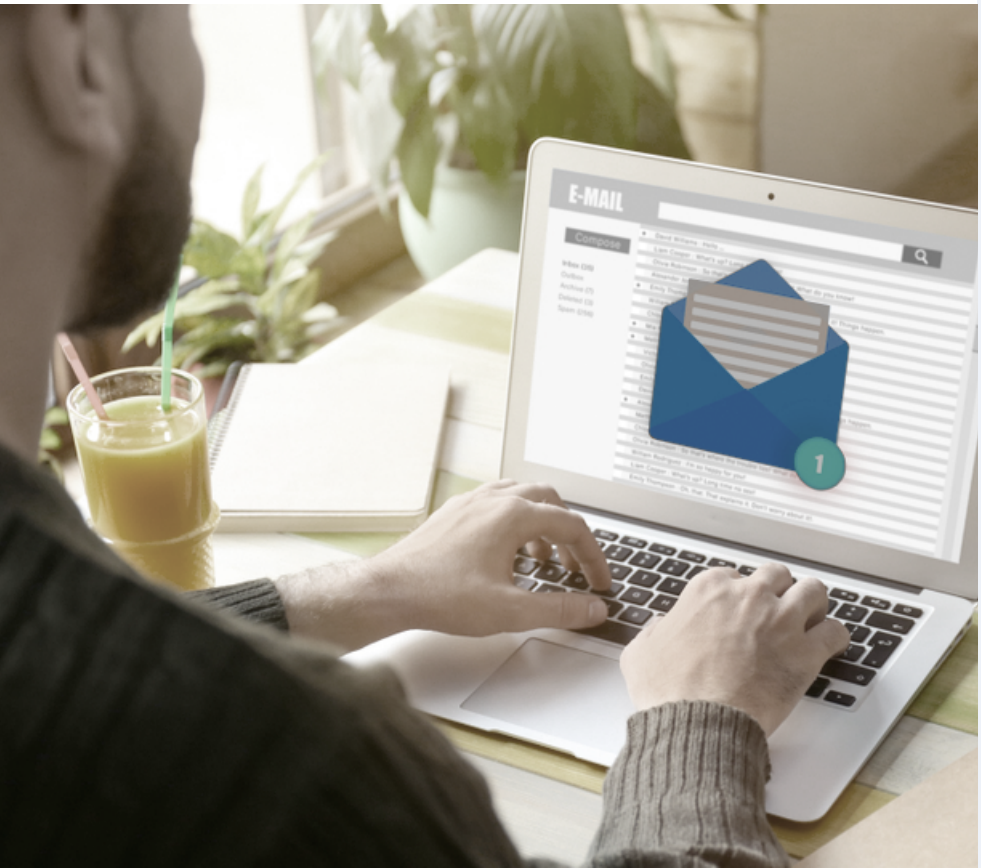
Benefits of a simulated phishing exercise?

- Test your security and improve your defenses
- Identify high risk areas that could lead to compromised systems
- Prepare your organization for a cyber-attack attempt
- Familiarize your team with the skills needed to detect and respond to an attack
- Decrease your chances of being victim to a ransomware or malware attack
- Evaluate the effectiveness of your security awareness program
- Reduce the risk of exposure to data loss, financial fraud, and embarrassment

steal sensitive data but also directly for financial gain, diverting funds from an organization. Traditional email inspection techniques can sometimes be ineffective at detecting phishing attacks because they resemble regular email content.

Understanding the critical role that they play in securing your business is a first step in strengthening your defenses. One way of doing this is testing the responses of your employees to a simulated real-world attack to gain an understanding of their level of vigilance as well as your level of exposure.

Advantio offers a range of phishing campaigns and awareness courses which are tailored to the individual needs of an organization. These exercises aim to make users more secure by testing their reactions to simulated attacks, creating awareness of real-world threats and educating them about the necessary responses to keep them secure.



5 Best Practices

Here are the top 5 best practices to embrace when carrying out the process:

Have explicit goals before starting

Get the executive team involved

Decide 2-3 behaviours you want to shape and work on those for 12-18 months

Treat your program like a marketing effort

Phish frequently, once a month minimum

What's involved in a Phishing Campaign?

Advantio offers a variety of phishing campaigns depending on the number of users to be targeted and the level of sophistication of attack that you would like your organization to be tested with. In all cases, phishing exercises are customized specifically for your organization including the sender information, email contents and organizational details.

As part of a phishing campaign, phishing emails of varying sophistications are crafted and sent to your chosen employees by Advantio's expert ethical hacking team. The interaction levels are benchmarked, and their engagement is tracked in order to build a picture of the level of awareness they have to this type of threat.

These emails are constructed in many formats and from varying senders to appear as legitimate as possible, appearing in many cases to be sent from within your own organization. We use a range of targeted topics to encourage interaction. The emails may appear:

- As an email from a colleague in your organization requesting information
- As an email with an attachment such as a word/excel file with macros
- As an email with links for users to click

Testing is conducted at 3 levels of sophistication:

We work with every organization to devise a program that suits the needs of their business based on the below 3 levels. In many cases, organizations may opt to run a program that covers all three levels for a select targeted group of users.

Fundamental
Phishing Campaign

Phishing emails of a common sophistication seen within the industry are sent to users and their responses are reported on. These emails take the form of widespread industry phishing types that employees may be susceptible to within their roles.

Intermediate
Phishing Campaign

More elaborate email phishing templates are used to test employee detection skills. These templates are more technically complicated with the aim of being more difficult to spot than the classic common phishing emails.

Advanced
Phishing Campaign

Uses 'spearphishing' to test a small number of staff with targeted emails created specifically for them based on knowledge collected by our ethical hacking team. We aim for as much personal info as possible to further infiltrate your organization.

These phishing exercises can be run independently or can form a critical part of a wider Red Team engagement. The purpose of this is to gain access to a user's account or physical location through reconnaissance.

Reporting a phishing attack

In addition to testing the response to phishing emails, we encourage organizations to monitor the levels of reporting by users during phishing exercises. This will enable us to understand whether recipients know what to do in such a case.

What is Spearphishing?

Our Advanced campaign uses spearphishing techniques to test individuals with personalized and well-informed content to trick the user into believing the email is legitimate.

Information is gathered by senior Advantio ethical hackers using a technique called OSINT (Open-source intelligence) which consists of searching public information such as Google, LinkedIn, Facebook, Instagram, government reports, data leaks, newspapers, etc. to build a picture of specific users. The aim is to find out as much about a user as possible such as what they like, where they work, which bank or mobile phone company they use, etc. - all information that may possibly help to prepare a personalized targeted phishing email which is complicated to detect.

What you receive from the exercise

Once our phishing exercise is complete, a comprehensive report is prepared for the organization outlining the statistics from the campaign and highlighting the security issues uncovered.

The findings are assigned a risk rating and evidence is provided to support all findings. Best practices are shared by the Advantio team to support the organization in building an awareness programme for its users.

Phishing awareness training

It is important to follow up a phishing exercise with user awareness training to ensure that your users become aware of the potential impact and implications of their interactions and understand that phishing is a real threat that they may be exposed to.

The aim of awareness training is for users to feel empowered to react to a similar phishing situation in future and gain the confidence to know how to react if they believe they encounter a phishing email.

Where requested, Advantio can develop an awareness training programme to support the findings of the test. This is fully customizable to the organization and is delivered by the Advantio ethical hacking team.

In addition to recognizing user involvement in a phishing attack, simulated attacks also allow your organization to take steps to optimize your technical defenses for real-world attacks and to take action to enhance your policies, processes and toolsets to ensure that similar phishing emails don't evade technical defenses.

Did you know?

According to the Cost of a Data Breach Report 2022, phishing was the costliest initial attack vector of a breach averaging USD 4.91m in breach costs. Breaches caused by phishing had a mean time to identify and contain of 295 days.

5 ways to protect your organization from the threat of phishing

1. Take part in regular phishing exercises to simulate attacks and test your ability to respond
2. Carry out regular security awareness training with your employees
3. Ensure your email gateway solution is secure and includes advanced phishing protections
4. Implement domain-based message authentication, reporting and conformance (DMARC)
5. Implement Multifactor authentication so account take-over is not possible

Compliance Requirements

PCI Security Standards Council™

Many regulatory frameworks require security awareness training to be conducted in order to be compliant.

PCI DSS 4.0 requires that security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to phishing and related attacks and social engineering (12.6.3.1). The standard calls out for good practice as having an effective security awareness program which includes ‘examples of phishing emails and periodic testing to determine the prevalence of personnel reporting such attacks’.

Why Should Your Organization Simulate a Phishing Attack?

Even some of the largest enterprises globally have fallen victim to a cyber-attack through phishing. Here are some of the most recent and notable phishing attacks globally:

2022 — Rockstar Games

Rockstar Games' upcoming title *'Grand Theft Auto 6'* suffered from leaked gameplay footage by a hacker on September 2022 as confirmed on Twitter

2023 — twitter

Data of over 200 million Twitter users was released in full on BreachForums on January 4th 2023 after a string of ransom attempts and leaks in December 2022

2023 — RIOT GAMES

In January 2023, Riot Game's legacy anti-cheat platform and two of its most popular games were exposed in a social engineering attack

2023 — PayPal

Approximately 35,000 customers had their accounts improperly accessed by Paypal in January 2023. Credential stuffing was involved in this incident

2023 — norton

Cybercriminals broke into users' accounts using credentials obtained on the dark web in early 2023, according to Gen Digital, Norton LifeLocks' parent company

Why clients choose Advantio

Advantio has become the trusted security partner of choice for hundreds of top tier companies and tens of thousands of small businesses globally. Advantio enjoys a 93% average retention rate of its clients who continue to place their trust in Advantio and value the company's expertise. Clients are based globally and typically have a specific focus in the Payment Card Industry but range across industry verticals including Financial & Payment Services, Hospitality & Leisure, Retail, Telecommunications, Government & Defence, Healthcare, Education, Travel, Technology, Infrastructure and Entertainment.

GET STARTED AT ADVANTIO.COM/PHISHING-CAMPAIGNS