OHPHISH

Fortifying Front Lines

EC-Council

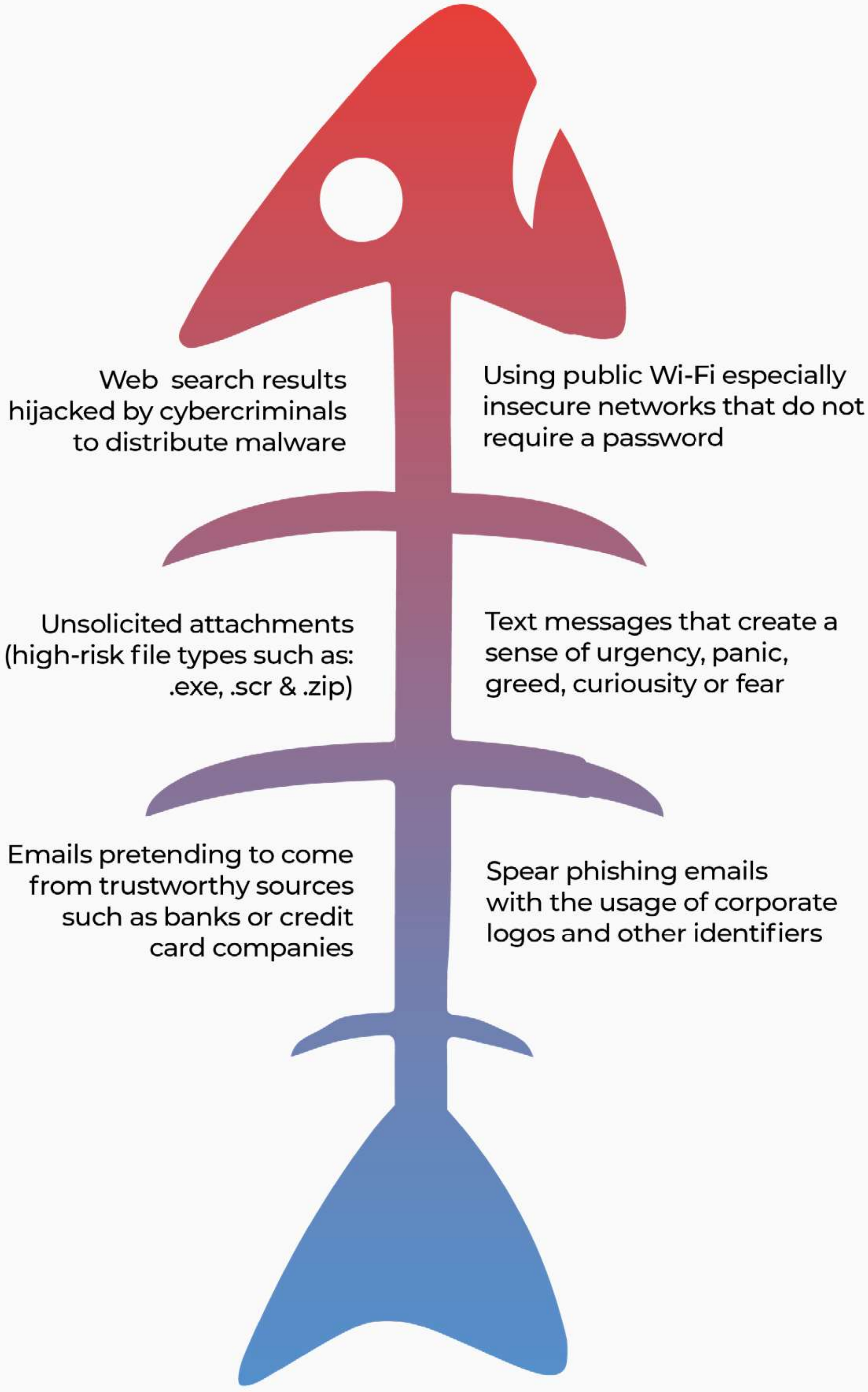
Secure your First Line of Defense

Studies show that 95% of cybersecurity breaches are caused by human error

Reduce the cyber risk to your organization with OhPhish. Our phishing simulations mimic real-life attack scenarios that teach your employees to spot phishing scams and avoid the hefty cost of a data breach.

Contact: ohphishsales@eccouncil.org | 800-813-0625

The 2 words Employees Should Not Utter After Clicking on a Phishing Email - OhPhish



Web search results hijacked by cybercriminals to distribute malware

Using public Wi-Fi especially insecure networks that do not require a password

Unsolicited attachments (high-risk file types such as: .exe, .scr & .zip)

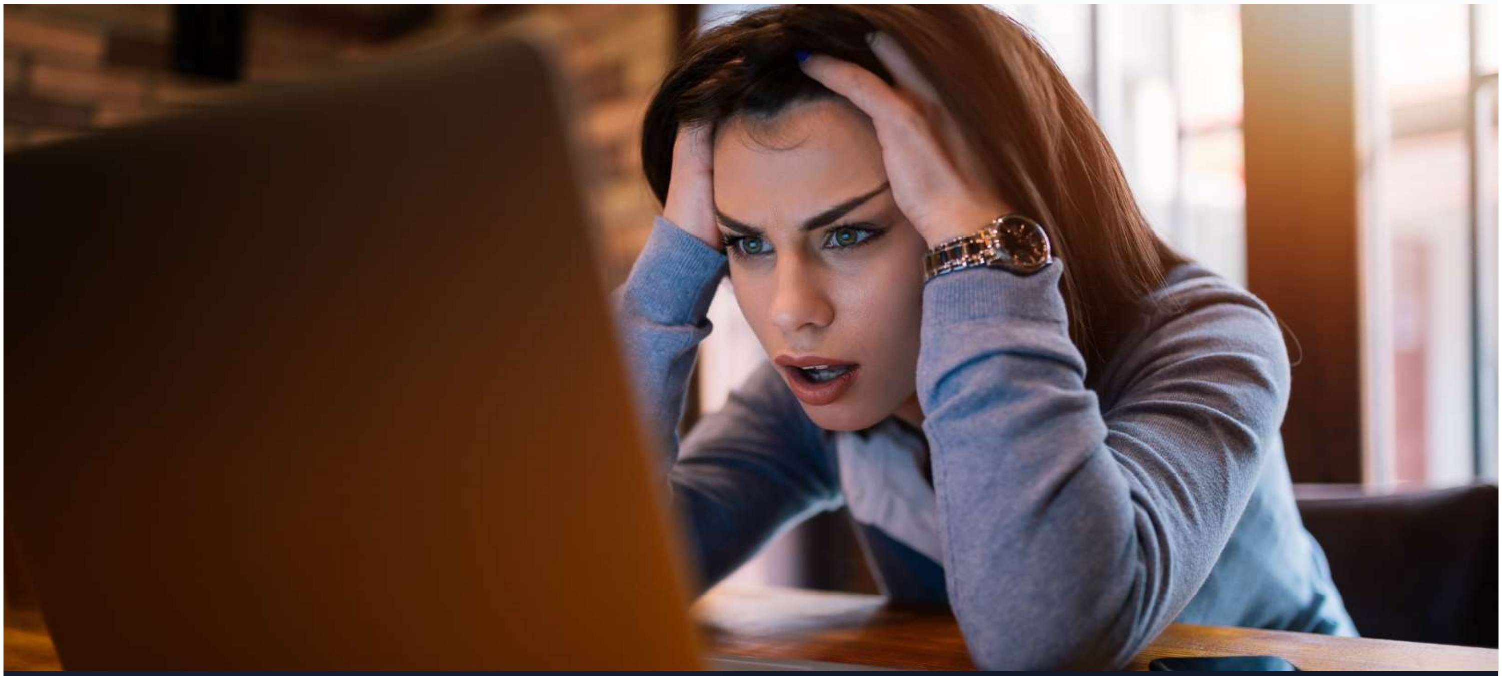
Text messages that create a sense of urgency, panic, greed, curiousity or fear

Emails pretending to come from trustworthy sources such as banks or credit card companies

Spear phishing emails with the usage of corporate logos and other identifiers

Ways You Could Get Hooked

Technology Alone Cannot Stop Humans From Clicking On The Wrong Links



01

Gone are the days when cybersecurity was the sole responsibility of the corporate IT department

02

Employees are vulnerable to malware through their use of company email, surfing the web, social media, instant messaging, or other network software

03

Employees must be able to recognize the types of attacks that may compromise company networks

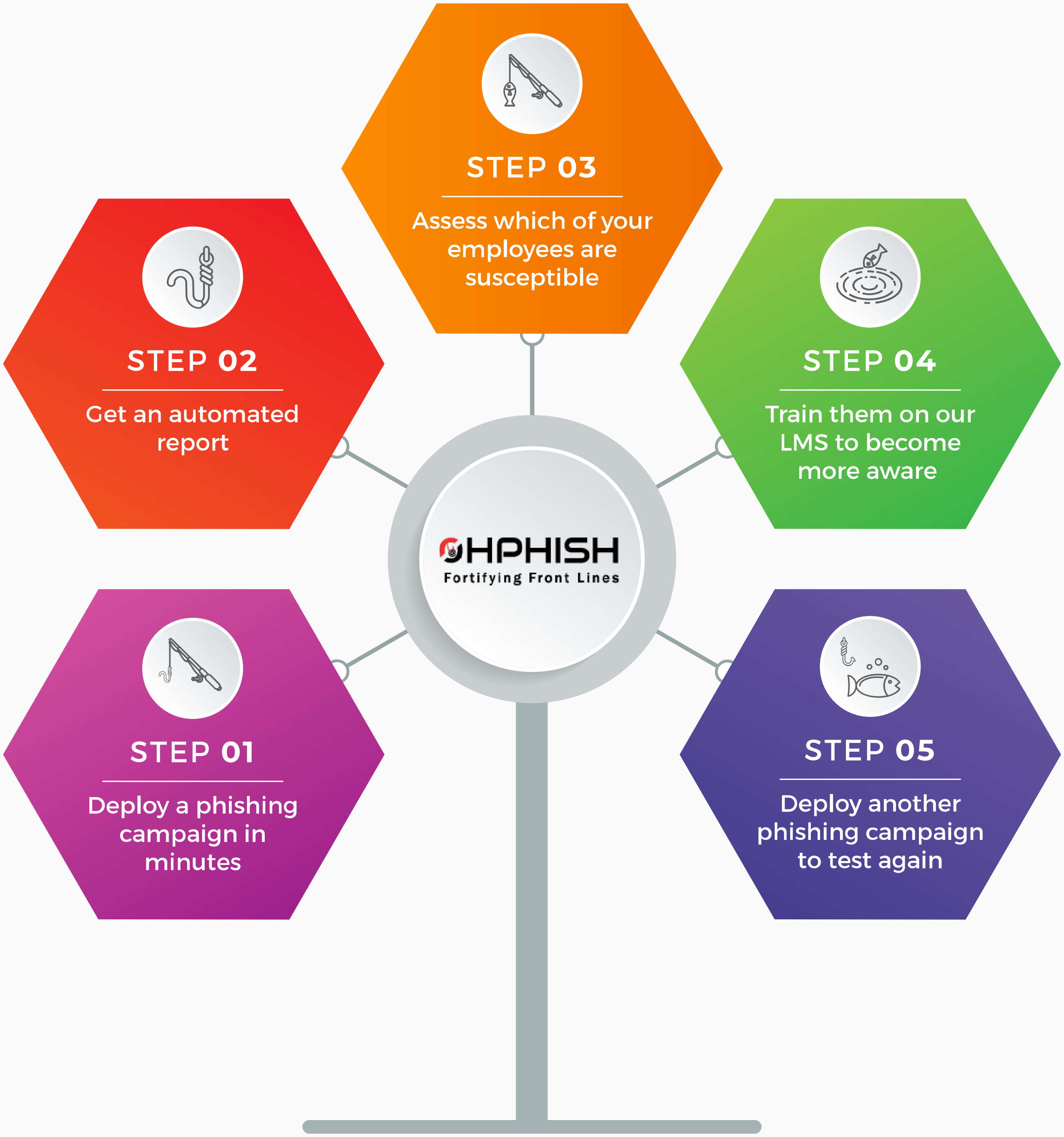
04

Staff must be prepared to use best practices against data breaches and malware infiltration as part of the organization's overall risk prevention program

Train Them to Think Before They Click

Research shows susceptibility to phishing emails drops almost 20% after a company runs just one failed simulation. Through accurate training, people learn, security awareness rises, and risk is mitigated with an intelligent solution like OhPhish.

With OhPhish, you can:



OHPHISH
Fortifying Front Lines

STEP 01
Deploy a phishing campaign in minutes

STEP 02
Get an automated report

STEP 03
Assess which of your employees are susceptible

STEP 04
Train them on our LMS to become more aware

STEP 05
Deploy another phishing campaign to test again

Repeat Steps 1-5 to raise awareness and dramatically reduce human error

An Employee Received a Phishing Email - Now What?

Dealing with the repercussions of a phishing attack is time consuming and costly. One careless click has the potential to compromise your entire network, so it is important that everyone works as a team to protect the company .

- Establish a system to report attacks, and emphasize to all of your employees the importance of following through with your IT deparment.

- Train your employees to contact your IT department immediately so that IT can take appropriate action and create a feedback loop to help improve the email filter.

- While structured annual or semi-annual training is recommended, employees should also receive on-the-fly training when an attack occurs.

- If an employee clicks on a phishing link, they should receive immediate feedback and additional training.

- Review the email with your employee, show them the red flags and indicators were missed, and provide additional training materials to help avoid being phished in the future.

OHPHISH
Fortifying Front Lines

An EC-Council Company

At OhPhish, we believe mitigating cybersecurity risks, especially those involving human error, begins with changing the cybersecurity hygiene of end-users. Our solution, which combines simulated phishing attacks with set-and-go training modules helps to improve awareness, alter user behavior and reduce the risk associated with social engineering attacks.