ETHICAL HACKING · BROCHURE

Are your employees ready to face attacks designed to harvest sensitive information?

Find out with an Ethical Phishing campaign

CYBERFERO

What is phishing?

It's a form of **online fraud** in which authentication credentials are stolen by tricking the user into entering them on a **fake page** that looks identical to a legitimate service the recipient actually uses.

Phishing attacks of this kind are **hard to detect automatically**, because the links in the emails may look legitimate to a machine.

The only way to avoid being fooled is to **know which signals to watch for and to stay alert at all times**. That's why it's so important to work on your team's resilience against these attacks.

If your employees can spot attack attempts, your company's data will be far safer.

> *The easiest element to hack is a distracted or naive employee. Giving them the right tools protects them — and the whole company.*

The numbers are alarming

96%
of attacks arrive via email

2M+
active phishing sites

$80K
average loss per company

69%
of breaches caused by employees

The benefits of an Ethical Phishing campaign

01

Test your corporate defences

We test your employees by sending messages identical to a real *phishing campaign*, but in a **controlled environment**, never putting the company at actual risk.

We collect responses and analyse them to produce a report and **targeted training**.

02

Analyse the results

The *Ethical Phishing* campaign produces **detailed reports** containing essential information to identify weak points across the tested scenarios.

Some of the information collected: number of message opens, number of clicks, which credentials are used, etc. The data also quantifies **user awareness** in recognising suspicious emails.

03

Train employees in a targeted way

Run a **training and awareness campaign** on cybersecurity for your employees.

By running the *ethical phishing* service and using the results to personalise the training programme, the intervention becomes **far more effective**.

Methodologies we use

Credential harvesting

This type of *phishing* leverages direct attacks on people who aren't fully aware of **hacking techniques**.

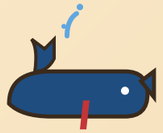
We get employees to reveal their credentials themselves.

Ideal for assessing **how susceptible your employees are** to *phishing* attacks; the collected credentials can also be reviewed to ensure they comply with a **sound password policy**.

Spear phishing

In this case the attack is aimed at a **specific target group** of individuals (e.g. the finance department).

The attack uses **information specific to the target** or targets, making the *phishing* attempt far more credible and selective.



Whaling

The attack target sits at the **executive level** within the organisation.

These targets are particularly sensitive because, once compromised, they can **exert significant influence** over other employees — amplifying the damage of the attack.

Our approach

Goals to reach

Running an *Ethical Phishing* campaign means uncovering the **weak points** of the company through the attacker's eyes — with the ultimate aim of performing a **true simulation of a cyber attack**.

What we're looking for

The campaign aims to find out **how susceptible and "fool-able" your employees are** to scams delivered through digital channels. We'll learn how reluctant they are to share **personal information, access codes or financial data** belonging to the company.

What we'll do

The *phishing* activity can include phases of **Social Engineering**, sending messages or even **trap phone calls**, aimed at gathering sensitive information or personal data that an attacker could use.

What to expect afterwards

After the campaign and the resulting **targeted training**, your employees will be able to defend the company **simply by ignoring** suspicious messages — we give them the tools to recognise them.

The best defence against phishing is knowing how to recognise it.

Since **2011** we've been working in Cloud technology and cybersecurity — rely on experienced professionals.

Choose security for your business

Discover the service on our website

CYBERFERO

For more information, our contact details are:

Via Statuto 3,
42121 Reggio Emilia (RE), Italy
www.cyberfero.com

Phone: +39 0522 1685330
E-mail: info@cyberfero.com
PEC: cyberfero@pec.it
VAT ID: 03058120357