# SECURITY AWARENESS TRAINING FOR EMPLOYEES

## An advanced approach against Client-Side attacks, by ISO Cyber Academy

*ISO/IEC 27001 compliant*

- ✓ *Interactive training programs*
- ✓ *Live hacking demonstrations*
- ✓ *Practical ''danger zone'' exercise*
- ✓ *Knowledge check*

---

*Suitable for any company size and industry*

## Client-Side attack

Compared to server-side attacks when the hacker exploits the vulnerabilities of a system and needs the IP address of the target, the client-side attacks require a direct user interaction such as opening a link or attachment, without knowledge of an IP address. The user is tricked into visiting a specially crafted link or opening an attachment that contains a malicious code or program. In this way, the victim's machine gets infected with a ransomware, backdoor, keylogger, viruses, and other malicious programs.

## Why a client-side attack will always be successful, unless...?

Companies' heavy reliance on technology to protect against evolving cyber threats ignores a critical element – the human element. After avoiding the antivirus, a hacker will get through your user. The attempts can be prevented only if you transform your users into a strong control against client side attacks, by teaching them how to recognize a phishing attempt, avoid the infection while browsing and report if any incidents took place.

## How do we help in preventing Client-Side attacks?

*We will know how to prevent cyber threats against us, only if we understand the hacker's mind set and the tricks used to gain access to our computers*

### Training program description

Our security awareness training is designed to raise the awareness of the most dangerous cyber threats to which users are exposed daily while at work or home. The purpose is to improve the internet security literacy of the employees, show the consequence through real time hacking demos and teach them how to avoid falling victim to cyberattacks**.**

### Why our training programs are effective?

We use advanced learning methods that make our training programs substantially different from the classical pre-recorded video training on information security. Combining **live hacking demonstration** with a practical threat based approach and ''danger zone'' exercise, we help companies strengthen their user level security, in the most effective way possible as of today.

## After the training, the employees will be able to:

- ✓ Understand their role in protecting information security in the organization
- ✓ Describe common ways criminals try to gain access to their PCs and consequently to the company's network
- ✓ Identify red flags that alert them to the danger of an attack while browsing
- ✓ Find red flags in a typical phishing email
- ✓ Prevent client-side attacks
- ✓ Adopt a new behaviour and mind set in term of internet security
- ✓ Adopt terminology related to cybersecurity

## How is the security awareness training structured?

The explanations and live hacking demos are carried out following the strategic path built, typically, by a hacker to gain access to a computer

I. THE CODE

II. DELIVERY METHODS

III. POST EXPLOITATION

## First, the hacker must create a code/program needed to perform the attack and make sure it bypasses all antivirus programs

- Here we explain the most common malicious codes and programs used by a hacker while performing a client-side attack (keyloggers, backdoors, ransomware, etc). What are these and why would a hacker want to have it served to the user?
- We show how a backdoor takes the shape of a JPEG image, a PDF file or any other file type to trick the user into believing that this is a legit file and open it. The students learn how to recognize a malicious file and prevent it from being executed.
- We demonstrate how a backdoor bypasses all 35 major antiviruses.

## The hacker must find a smart way to deliver the malicious code or program to the victim

- If in the previous section we show how a malicious file can bypass the antivirus, here we explain how it bypasses the user (the employee). We show how a hacker uses Social Engineering and various smart delivery methods to install malicious programs on their computer.

- We explain what are the ‘’red flags’’ in a phishing email and how to recognize a phishing attempt while browsing.

Here are some examples of the threats we explain and demonstrate:

## ✓ Phishing and spear phishing

1. Link manipulation

a) IDN homograph attack. Example: http://www.goog1e.com
b) Subdomains and misspelling
c) Hidden URLs. Example: click here

2. Email spoofing (the hacker sends an email containing an infected file or link, from any email account).
3. Examples of real phishing emails and red flags to watch for.

- ✓ **Information gathering.** How does a hacker use publicly available information to build the strategy of an attack against a company exploiting the users' weakness? Why protecting the data about your social network accounts and emails is important?
- ✓ **The danger of Wi-Fi**. Connecting to a fake access point in a coffee shop or airport: fake login prompt to steal passwords, google page spoofing, turning on the camera, fake updates to install a backdoor, etc
- ✓ **The danger of http** and https bogus certificates
- ✓ **The danger of a hooked web browser and XSS**
- ✓ **The danger of cookies.** How a hacker gains access to your online accounts without any login credentials.

Now that we saw how a hacker can have the malicious code or program executed on the victim's machine, we show the damage that can be done.

- We show the hackers screen after gaining a full access to the machine and the commands that can be run: open or download any file on the hacked computer, upload any new files containing viruses, deleting files, take screen shots, turning on the camera, keylogging etc).
- Explaining the pivoting: how a hacked computer can give access to the entire network
- We answer such questions as ''If I delete the infected file on my PC, is the hacker still going to be able maintain control over my PC. Will still the hacker be able to maintain the access if I restart or shut down the computer?

| | |
|---|---|
| Password security | Social Engineering |
| Media drop | Safe browsing |
| Mobile security | CEO Fraud |
| SMishing | User liability |
| Vishing | GDPR |
| Phishing | Ransomware |

For more details please contact our team at office@isocyberacademy.com