Social Engineering

Criminals often use social engineering to gain access to systems. They "hack people" to obtain sensitive information. If your employees are aware of this, you reduce the risk of serious cyber incidents. We can help raise awareness with phishing simulations and other Social Engineering Services.

These Social Engineering Services give you:

Insight into vulnerabilities

These services show you how resilient your employees are against social engineering.

Aware employees

By allowing employees to experience simulated attacks, you increase their awareness.

A partner with expertise

Our ethical social engineers have extensive experience and operate with care.

Why choose Social Engineering Services?

The technical security of systems is improving all the time. To still gain access to your networks and systems, cybercriminals use **social engineering**. They impersonate someone else and manipulate employees into handing over sensitive data. The best-known form is e-mail phishing, but social engineering can also be done by phone or physically. It is important that your employees are aware of how social engineers operate.

The first goal of these Social Engineering Services is to test which business information an attacker can uncover. We have multiple ways to do this, from physical or telephone social engineering, to e-mail phishing simulations. The second goal is to make your employees aware of the risks of social engineering. Higher awareness reduces the likelihood of a serious security incident within your organization.

The Social Engineering Services we offer:

- E-mail phishing simulation
- Telephone phishing
- Phishing Specials (smishing etc)
- Mystery Guest assessment

E-mail phishing simulation

Email phishing is the most commonly used way by cybercriminals to gain initial access to a network. To alert your employees to these fake emails, we conduct an email phishing simulation. The goal of a phishing campaign is always to positively influence employee awareness, attitudes and actions.

In close consultation with you, we set up an email phishing campaign. During an agreed period, we **send simulated phishing e-mails** and measure employee response: do people click on the link in the e-mail? Do they report the phishing e-mail to the designated contact point?

At the end of the campaign, you receive all metrics in a report. We provide you with **concrete recommendations** so you can take action to increase your resilience against e-mail phishing.

Telephone phishing

Telephone phishing involves criminals posing on the phone as an IT helpdeks assistant, for example, in order to extract sensitive data from people. During a telephone phishing assessment, our social engineers phone a number of your employees to check how resilient your organization is against this kind of attack. You receive anonymized video footage of the investigation that you can use to train other employees. This is an effective learning method.

How telephone phishing works

1	The social engineers call a number of your employees on a specified day. In 2023, they phoned around 400 people.
2	During the phone call, they try to persuade your employees to give sensitive information. They succeed on average in 1 out of 3 cases.
3	Immediately after the interview, there is a so-called ‘debrief’. Our social engineers explain what they have just done to your employee.

Phishing Specials

Besides e-mail phishing and telephone phishing, cybercriminals also use other forms of deception, for example, phishing via SMS, or ‘smishing’. You can employ our social engineers for the following tactics to test your resilience:

With **USB phishing**, attackers leave or give away a USB flash drive with malware on it. If someone plugs the USB into a computer, the attacker can gain access.

SMS phishing, or smishing, involves scammers sending fake text or instant messages. They pressure people with messages that appear urgent and then ask people to click on a link or share personal information.

QR phishing, or quishing, uses QR codes that lead to a malicious website after scanning. Scammers try to trick people into scanning this QR code, with the aim of stealing personal information or installing malware.

Mystery Guest Assessment

During a Mystery Guest Assessment, our ethical social engineers try to gain physical access to your offices and premises. They then try to gather information present on desks and workstations, in documents, archives and on the internal company network, through workstations, printers or network connections.

The social engineers use an outlined scenario that they determine in consultation with you. This makes the assessment **as realistic as possible**.

With the results of the assessment, you can **improve the security** of your physical locations against unwanted visitors and train your employees.

What our clients say

“I won’t fall for this again”

“To be honest, we did not expect our employees to give this many passwords to social engineers over the phone. We hear back from employees, "I'm kind of shocked, but it's really good that you guys are doing this. I'm never going to fall for this again..’”

Related services

OSINT Assessment

OSINT is short for ‘Open Source Intelligence’: it is information from public sources such as social media and news websites. During this assessment, we check which information about your organization is publicly available online, so you can protect yourself.

Cybersecurity e-Learning

Do you want to give your employees up-to-date cybersecurity knowledge? We offer accessible and interactive Cybersecurity e-Learning modules, designed for effective knowledge transfer.

SAFE Awareness Program

The gap between security awareness and safe behavior is significant. That's why the SAFE Awareness Program focuses on actual behavior change. During this program, your employees receive training, interventions and tools to help them behave more securely so that your organization is better protected against cyber attacks.

Secura
A BUREAU VERITAS COMPANY

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Example case | Telephone Phishing

Which problem did the client have?

A Dutch municipality wanted to know if their employees were resilient to social engineering. So they asked us to conduct a telephone phishing assessment.

Result

Our social engineers called a number of employees and managed to get the password from many of them. An anonymous video of this phishing simulation was shared with all employees. This video received major attention throughout the organization, really raising the municipality’s security awareness.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

info@secura.com

+31 (0) 88 888 3100

secura.com