This is how a hacker can lure you into exposing your company to attacks.
A man wearing a suit and carrying a briefcase enters the building, appearing to be extremely busy. He walks to reception and introduces himself as a consultant working for a well-known global company. He explains that he’s late for a very important meeting.

The consultant doesn’t have an ID badge. But he mentions two employees of the company that he agreed to meet. The man emphasizes that he’s already late for the meeting, and begs the receptionist to let him in.

The receptionist tries to call the employees that the consultant mentioned, but neither of them answers the phone. That’s no surprise - both are on a business trip on the other side of the globe. The consultant explains that there’s a large sum of money at stake. This explanation, and the implied consequences of delaying the meeting, intimidates the receptionist into letting the consultant in the building.

In reality, the man in a suit isn’t a business consultant. He’s a cyber security professional trying to break into the company’s information...
It’s common knowledge amongst security professionals that regular people are the weakest link in cyber security. That’s why social engineering - the psychological manipulation of people into performing actions or divulging information - is a staple in Red Team exercises.

“Taking advantage of people’s goodwill is the most common trick hackers use,” confirms Janne. “The most important thing is to pinpoint the target’s weakest spots.”

It’s pretty common to contact victims by phone. In a typical phishing attempt, the caller pretends to be from the IT department and explains that he’s investigating a possible breach. To rule out the possibility, the “IT admin” will claim to need access to the victim’s computer. And that’s how user credentials get into the wrong hands.

“To date, our cyber security professionals have a 100% success rate in Red Team drills”

Janne Kauhanen, F-Secure Cyber Security Services unit

EXPOSING INFORMATION OVER THE PHONE? A BAD IDEA.

systems using any means necessary. It’s what’s called a Red Team – an exercise where cyber security professionals test customer organizations by trying to find vulnerabilities that can lead to data breaches.

Even though the example above is fictional, our security experts use similar tactics in real Red Team drills. Made-up stories and disguises are useful tools to access buildings that would otherwise be restricted to the public.
won a prize and have to hurry to redeem it. Because someone always stumbles.”

Another human trait that’s commonly exploited in social engineering is jealousy. According to Janne, a hacker can, for example, send an employee an email where he’s told that he’s been denied access to a workplace LinkedIn discussion group. This kind of interference can cause anger that leads the employee to click on a link in a phishing email. Clicking the link redirects the employee to a site that looks like LinkedIn, allowing attackers to discover the employee’s password as they try to log in.

“The most important thing is to pinpoint the target’s weakest spots.”

To tackle these kinds of issues, companies order test attacks from companies like F-Secure. In a Red Team drill, an elite team of trained professionals from our Cyber Security Services unit engages in an all-out attempt to gain access to customer systems.
Red Teaming is a concept with military origins. Defense forces use it to refer to adversary units in field exercises. Nowadays, the phrase is commonly used in cyber security.

The purpose of our Red Team exercises is to demonstrate how online crime, industrial espionage, and black hat hacking work in real life. The exercises are always ordered by customer companies.

“More and more companies are starting to wake up to the current reality where locked doors and guards in the lobby are not enough to secure organizations. Companies want to know how exposed they are,” Janne explains.

The specifics of the drill, as well as the objectives, are always agreed upon by both parties before any Red Team tests proceed. The target of the Red Team can be, for instance, to obtain the domain admin password of an information system that would give attackers access to the organization’s accounting and invoicing.

Our cyber security experts can also pick locks and break doors to achieve their objectives.

“We always agree with the customer in advance how much we can break things. For example, we agree beforehand if we can crack doors open if we need access to a company’s server room,” Janne reveals.

“More and more companies are starting to wake up to the current reality. Companies want to know how exposed they are.”

Even though lock picking is part of our Red Team’s tool set, it’s rarely needed. That’s because it’s usually very easy for an outsider to walk into a company’s premises – even in the middle of a regular work day.
Preparing a Red Team exercise always starts with inquiry. Just by browsing the web, our experts gain access to a large amount of useful information about the target organization. This could include, for example, information on the company’s premises, as well as contact information and photos of employees.

After conducting background research online, the experts start exploring the surroundings of the organization’s office building. First, they check whether the company’s wireless networks work from outside the office building. All it can take for a hacker to break into a company’s systems is a Wi-Fi signal that extends to an adjacent parking lot.

“We might even fly a drone up to the roof of a building that has a router inside, and use that to sign in to their Wi-Fi network,” says Janne.

If breaking in to the company wireless network doesn’t work, the experts start monitoring the company. During this phase, our experts pay special attention to the organization’s employees. This can include their online and offline behavior – how they dress, what time they come to work and leave the office, if they receive a lot of external guests, and so on.
Monitoring company routines can take several days or even weeks. Information gathered through reconnaissance is essential, as the Red Team doesn’t want to draw any special attention to themselves during their operations.

“We might even fly a drone up to the roof of a building that has a router inside, and use that to sign in to their Wi-Fi network.”

“In general, it’s pretty easy to infiltrate the staff of a large organization. Many people find it difficult to approach a strange person in the company premises. And even if they would, we usually have a solid cover story and a cloned ID badge with us. Talking to the employees of the company can even make it even easier for us to break in if we manage to make them reveal useful information to us,” Janne points out.

Once the Red Team has access to a company’s premises and identified the targets of a security breach, the real hacking can begin.

A computer doesn’t even need to be turned on for it to be vulnerable. A hacker that’s snooping at the office can, for example, insert a small keylogger memory stick in a computer’s USB port. Devices like these can use malware that starts to follow every press of a keyboard button.

“Very few people check the outside of their computer as they return to work in the morning. And if we want to be mean, we can also hide spying equipment inside computers,” Janne explains.

It’s not unheard of for people to leave their computers open and unlocked when they leave work. Alternatively, passwords can be found written on post-it notes under the keyboard, or in a drawer next to a desk. In many companies, confidential papers and materials are collected in locked trash bins, which can also become a security vulnerability if they are not properly taken care of and the papers inside regularly disposed of.
The tactics used in hacking and social engineering are becoming more and more advanced. How can you avoid being scammed? For a company, the key to managing security risks is to increase employee awareness about cyber security, and to provide comprehensive security guidance for all employees.

It’s crucial that this guidance is clear and unambiguous. If the receptionist of an organization has a strict policy not to let anyone in without an ID badge, and everyone follows the policy meticulously and without exceptions, it is difficult for intruders to get in. However, if exceptions to the rules are sometimes allowed, it’s more likely people will deviate from the rules based on their desire to be helpful to their colleagues.

Not everyone knows to be suspicious of memory sticks found in public places. And they don’t necessarily know that these devices can contain malware and should not be used.

When it comes to cyber security, maintaining healthy suspicion is very much recommended.

“Don’t stick your head in the sand. You always have to lock your computer when you leave it behind. I also recommend every employee use password tools available in the market, as self-generated passwords are often weak. You don’t want to make yourself an easy target, as that’s exactly what criminals are after,” Janne summarizes.

A HEALTHY DOSE OF SUSPICION CAN GET YOU FAR

“You don’t want to make yourself an easy target, as that’s exactly what criminals are after.”

This story is based on an article by the Finnish broadcasting company, YLE, published online on March 5, 2017.
CONSIDERING A RED TEAM EXERCISE?
LET US IN. KEEP THEM OUT.