issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Shut the Door

against Cyber Attacks on Small Businesses

Factsheet
Nº 3

issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Shut the Door

against Cyber Attacks on Small Businesses

Factsheet
Nº 3

A real-life example

The small historical restaurant named „Zum Lamm" with 20 employees is located at the centre of Bonn. It has been a popular destination for decades as this is the third generation of owners in the family. However, over the last 10 days, the restaurant remains closed, as its online booking system, computers and POs devices have become inaccessible. An IT contractor company has been called in and they seem to be making progress in restoring everything to how it was, but their cost was high, and the financial loss of business during these 10 days was even higher.

What happened?

A few days earlier the owner had received a very convincing email with an invoice attached supposedly from their trusted wine supplier. However, it turned out, it was a cyber criminal impersonating the wine supplier and the attachment was a computer virus, which had started deleting files and disabling computer systems, followed by a notification that the disruption will be permanent unless the owner pays up a ransom of €30,000.

This story sounds implausible? Similar incidents happen very often

DThis type of computer virus is called ransomware. When activated, it starts encrypting the files in a computer. This effectively makes them completely inaccessible, because only the cyber criminal has the "digital key" that can decrypt them. This is only one of the many different types of computer viruses that are used by cyber criminals.

This all sounds very technical and very worrying. The good news is that the most effective defence against cyber threats like them is actually neither technical nor difficult. The vast majority of cyber criminals depend on social engineering, which is about deceiving a human into making a mistake and allowing the cyber criminals access to their computer systems. They might send an email pretending to be from an organization that you trust like your bank or an online shop. They might send you a "by the way, check this link" text message followed by a link, using the name of a friend of yours, so that your mobile phone appends it in your existing discussion with your friend. They might share a screenshot of a video that looks too interesting to miss, and when prompted with a warning to install a special software update to watch it, you click because the curiosity is overpowering. In all cases, the cyber criminal wants to deceive you into making the mistake to ask your computer to install something that you shouldn't.

Basic cyber hygiene measures for protecting your company against social engineering

Realizing that one has been deceived is never a good feeling.

Also, everyone believes that they are too smart to be deceived. The reality is completely different. Even the most experienced cyber security experts and professors have been deceived and in some cases in very high-profile incidents. We are all vulnerable to deception. One of the most important reasons is that interacting with someone through the Internet is not the same as interacting with them in person. It is not easy to tell whether someone is lying if you cannot see them and if the email they send looks exactly the same as a real email would be from a person you trust. Nevertheless, there are ways in which you can improve your company's resilience to social engineering by taking a few simple steps:

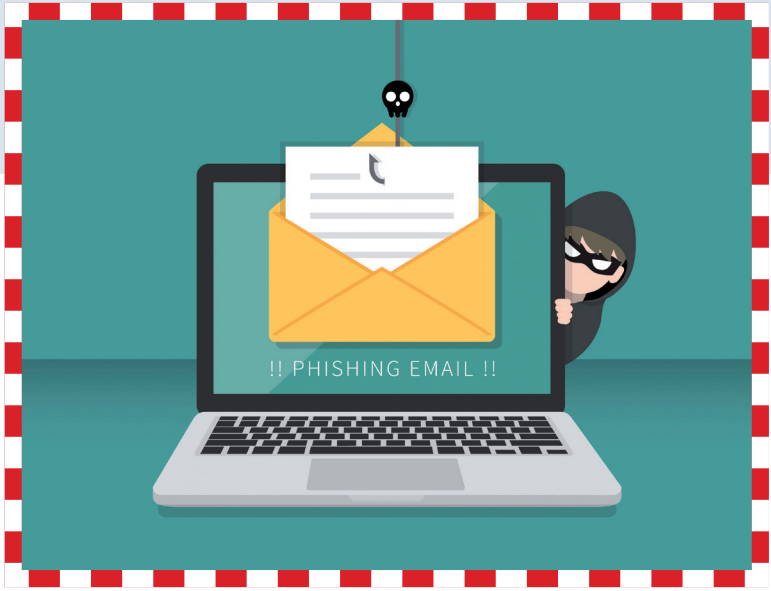
If something feels strange or too good to be true, chances are it is. For example, if you receive a notification for a purchase or a confirmation PDF that you never asked for, it may be worth making a phone call to the sender if they are who they claim to be.

Social engineering often relies on creating a sense of urgency, fear or other intense emotion. In such conditions, it is easy to make a mistake. Before clicking on a link or email attachment, take a moment to think. Consider asking your staff to take a security awareness training program. In almost all cases, cyber criminals re-use the same social engineering techniques to target companies. Simply knowing these techniques can help you in being more vigilant. It is an investment that may save you a lot in the long-run.

Limit the information you are releasing online to the minimum necessary. Social engineers routinely use online information, for example from social media, to make their messages to you appear legitimate. It is a good idea to develop a social media policy that takes into account privacy and prevents oversharing.

Consider adding two-factor authentication in all critical aspects of your company, such as access to customer data. In this way, if a password is compromised, it will not be enough for the cyber criminal to access your systems.

Make your staff "human sensors" and give them a sense of ownership of the problem of cyber security to the company. If they encounter a social engineering attempt against them, they should be encouraged to share this information within the company. They might have not fallen for it, but others in the company will be targeted by the same attack and they might fall for it if they are not warned.

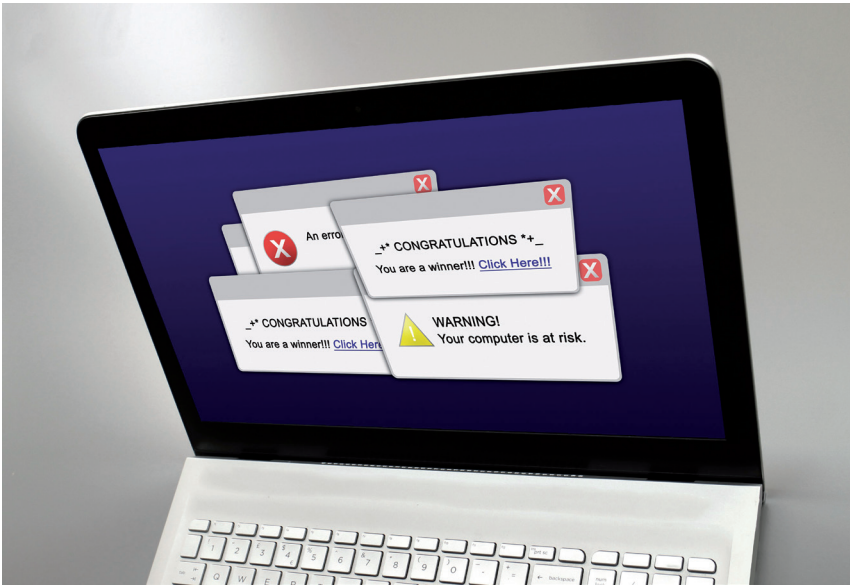


Further information

1 **What is social engineering?**
https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

2 **Phishing attacks: defending your organisation**
https://www.ncsc.gov.uk/guidance/phishing

3 **How to recognize and avoid phishing scams**
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams



6 tips for protecting your company against social engineering

1. If something feels to strange or too good to be true, trust your instinct.
2. Before clicking on a link or email attachment, take a moment to think whether you should.
3. Consider investing in security awareness training.
4. Limit what you post on social media to what is necessary.
5. Consider adding two-factor authentication to critical systems.
6. Ask your staff to report any social engineering attempt that they encounter.

issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

ISSA-Section
Machine and System Safety

Dynamostrasse 7–11
D-68165 Mannheim
Germany
Phone: +49 (0) 621 4456 2213
Fax: +49 (0) 621 4456 2190

www.safe-machines-at-work.org

AUVA

BGN
Berufsgenossenschaft
Nahrungsmittel und Gastgewerbe

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE
CONTRO GLI INFORTUNI SUL LAVORO

suva

TECHNICAL UNIVERSITY
OF KOŠICE

UNIVERSITY of GREENWICH