# Secure in the Home-Office with the CS-Method

More and more companies are offering their employees the opportunity to work from home. This creates more flexibility, but also brings challenges. The *CS-Method* relies to the *COMMON SENSE*. By using this method combined with the following 5 tips, you will make your contribution to working safely from home. The great thing is that not only your business but also you and your family will benefit from creating a cyber secure home.

## You are the „First Line of Defense“

Technology alone cannot fully protect you from cyber attacks - YOU are the best defense. Cyber attackers know that it is easier to attack you instead of your computers and other devices in order to get to the desired target. Cyber attackers, for example, specifically exploit stress situations to persuade their victims to take actions that they would not otherwise be tempted to take. Cyber criminals use various tricks to try to get your data or passwords by phone or email. They slip into the role of others, adopt the company jargon in order to appear as credible as possible or create artificially induced problems and then offer assistance.

If possible, you should therefore also adhere to the same security guidelines at home as those that apply in the company. Report information security and privacy incidents as appropriate immediately to the competent authorities.

Indicators for social engineering attacks are:

| | | |
|---|---|---|
| Someone is trying to get you to act by creating urgency through fear, intimidation, a crisis or an important appointment.<br>*In unusual situations, do not always respond immediately to every request. If you were called, make a note of the phone number and offer an immediate call back.* | You will receive an unsolicited email with the aim of clicking on a link, opening an attachment, checking or entering your personal data.<br>*Ignore such e-mails and if you are unsure, it is best to ask the sender on an alternative way.* | A friendly support engineer will contact you to perform important maintenance or installation work on your system and ask you for your password or for installing a program so that the support can be handled remotely.<br>*In such cases, do not comply with the requests and contact your IT department immediately and report the case.* |

## The Home-Network

You probably have a WiFi-enabled Internet router in your house. To enable your devices to connect, these routers constantly send out a WiFi signal. As a result, in most cases a connection to your WiFi network is possible 24 hours a day - unfortunately mostly beyond your own four walls.

This makes it especially important to secure WiFi networks well.

| | | |
|---|---|---|
| Depending on how remote access to the corporate network has been set up, you should use the web browser and email client in the respective remote connection to your company if possible, as this will allow your organization's protection systems to take effect. | You should make sure that only trustworthy people connect to your network. Create complex WiFi keys to protect your WiFi network from unauthorized access. Most WiFi routers already support options for setting up a guest WiFi and isolating connected devices. | Always change the default password of your network devices and do not use the administrator password of your wireless router as the wireless key. |

Dieses Factsheet wurde inspiriert durch den SANS Security Awareness Work-from-Home Deployment Kit

| | | |
|---|---|---|
| | *If you need assistance, your Internet service provider may be available to help you.* | |

## Passwords

Weak passwords are the achilles heel of a company's information security. In many cases, attackers can either guess passwords themselves or use simple programs that test frequently used passwords until the right one is found. Badly chosen passwords often lead to entire companies are being compromised. It is therefore particularly important to choose strong passwords.

It is best to think of a toothbrush when taking the password:

- you should choose a good one
- you should change her regularly
- you shouldn´t share her with somebody

So when choosing a password, pay particular attention that

- *NEVER* use the *same* password across multiple systems
- use a passwort-manager, also called a password-safe, to store passwords
- don´t use password combinations like 1234, QWERTY, ASDFG and so on
- name of pets, relatives, children, etc. and date of birth are NOT used
- *DO NOT* choose passwords that appear in dictionaries
- depending on company guidelines, at least 12 characters consisting of upper/lower case letters, numbers and special characters are used
  (above all, the length of the password plays a role - *THE LONGER, THE BETTER*!)
- the password is *NOT* shared and *NO* information about the composition of the password is shared
- according to company guidelines the passwords are changed regularly or *IMMEDIATELY* in case of compromise

## Updates

You should ensure that your computers, mobile devices, programs and apps are kept up to date. Cyber criminals are constantly trying to find and exploit vulnerabilities in systems. If devices, programs and apps are regularly updated, it becomes much harder for criminals to attack you in this way. If possible, activate automatic updates so that they are automatically installed on your devices. This rule applies not only to corporate devices. It applies to all technologies that connect to the Internet like Smart TVs, surveillance cameras, game consoles, internet enabled baby phones, heating control etc.

## Children and Guests

Just as in the company, it must be ensured that no other persons use the systems with which company data are accessed. In the home office, this mainly affects family members, childrens and guests. They must be made aware that company equipment may not be used because data may be accidentally deleted or modified or devices could be infected. Under certain circumstances, this would lead to serious information security or privacy consequences.

Dieses Factsheet wurde inspiriert durch den SANS Security Awareness Work-from-Home Deployment Kit