# Security Awareness


AWARE OF A (POSSIBLE) CYBER THREAT?
**CALL: (040 214) 2301**

# How you can help protect confidential information

**Dealer details, customer names, product development at DAF: during your work you are constantly in contact with information about the company and its personnel. Some of that information is freely accessible and available, while some of it is strictly confidential. It is very important that confidential information is protected. This is also your responsibility.**

We are often aware of external security threats, such as cyber attacks and viruses, but not everyone is aware of the 'internal' threats we sometimes face that are often the result of human error and/or carelessness. The aim of this brochure is to help you handle digital information in a safe manner so that we can deal with external and internal security threats.

## PROTECTING YOUR LAPTOP

Do you have a company laptop? Fortunately, you don't have to do much to protect it yourself as many different measures have been implemented to protect laptops against unwanted interference. For instance, our IT Department ensures that your laptop installs all updates automatically, blocks suspicious websites and malware as much as possible and instructs you to change your password regularly.

**There are extra steps you can take to protect the digital information on your laptop:**

- Check the security of the websites you visit. The URL should begin with https://.
- Be careful about connecting hardware that is not your own, such as USB sticks, to your laptop.

- Lock your laptop every time you leave your desk with Windows Key + L
- Shut down your laptop before closing it at the end of the day.
- Beware of e-mails with links and attachments from unknown senders and do not open them if it seems suspicious.

## REMOTE WORKING

Do you sometimes work away from the office? In that case it is wise to take extra precautions. Never leave your laptop unattended, do not connect to unknown or public WIFI networks and use PACCAR VPN. You should only save important documents on your OneDrive or S-Drive and not on your laptop. This ensures that these documents cannot be accessed by others when you are not connected to the secure DAF network and benefit from better protection as a result.

## SHARING INFORMATION

Sometimes you may be required to share confidential information with customers, business partners or suppliers. In that case they must first sign a non-disclosure agreement (NDA). Consult your contact at Purchasing or a colleague at Legal Affairs. They will draw up an NDA that can be signed by the other party. Protecting confidential information is a two-way street. We do not provide others with confidential information or, conversely, accept confidential information from others without due consideration. In the latter case it is always wise to first seek approval from our legal department.

## SOCIAL MEDIA

Social media have become part of both our personal and professional lives. Most of us use LinkedIn for job-related matters, but you may also have a personal Facebook or Instagram account. You are responsible for your own online activities, but your personal accounts can also have an effect on DAF Trucks. Others can easily access information about your employer and

job-related matters and use it to their advantage. Those whose intentions are less than pure can identify your location via your posts on social media and this can also present risks for yourself, such as the possibility of your house being burgled when you are away on holidays.

**You can protect both your personal and professional information on social media by adhering to the following:**

- Do not accept friendship or connection requests from people you don't know
- Restrict access to your social media profiles by unknown parties
- Never share your location on Facebook or Instagram

The sharing of confidential company information or competitively sensitive information on social media is not permitted. This doesn't mean that you can never make any reference to your work on social media platforms. Always think twice before posting on social media and if you are not sure whether or not you may post something, ask your supervisor.

**AWARE OF A (POSSIBLE) CYBER THREAT?**

A cyber security threat can come in many forms: an e-mail from a suspicious source, a notification on your laptop that you have never seen before or a dubious URL. When in doubt, always contact the IT Service desk at (040 214) 2301.