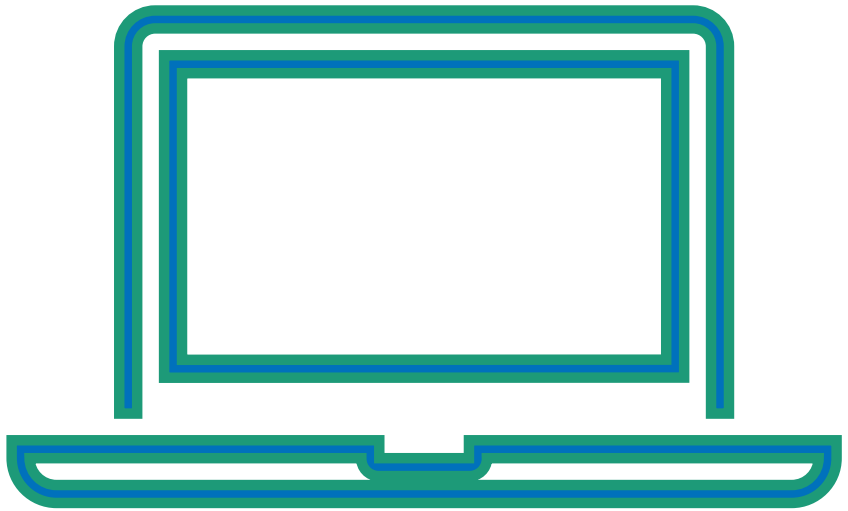

TRUSTED COMPUTING LTD
STRAIGHTFORWARD TECHNOLOGY

5 THINGS YOU SHOULD NEVER DO ON A WORK COMPUTER

AND WHY!

What's the harm?

No matter how convenient, it's a really bad idea to use your work PC for personal tasks.

Many employees are blissfully ignorant of the strict IT policies that are typically built-in to employment contracts / company handbooks - usually with disciplinary sanctions for breaches.

Those same policies also serve to protect you, as you might inadvertently be allowing other people access to your personal data and accounts.

Read on for 5 things that you should never do on your work computer.

1. NEVER SAVE YOUR PERSONAL PASSWORDS IN THE BROWSER

Many people keep track of their passwords by letting their browser save them and then fill them in automatically. This can be helpful, but if you lose access to that PC, it's not very safe.

When the computer you use isn’t your own, it can be taken away at any time for all sorts of reasons, such as an upgrade, repair, or during an unexpected termination. If someone else accesses that device and you never signed out of the browser, that means they can leverage your passwords to access your cloud accounts.

Not all older PCs are stored safely or destroyed. Some companies will donate them to worthy causes, which could leave your passwords in the hands of a stranger if the PC hasn’t been wiped properly.

2. NEVER STORE PERSONAL DATA

It's very easy to get in the habit of storing personal information on your work computer, especially if your home PC doesn't have a lot of storage space. But this is a bad habit and leaves you wide open to a couple of major problems:

- Loss of your files: If you lose access to the PC for any reason, your files can be lost forever
- Your personal files being company-accessible: Many companies have backups of employee devices to protect against data loss. So, those beach photos stored on your work PC that you'd rather not have anyone else see could be accessible company-wide because they're captured in a backup process.

3. NEVER VISIT ‘SKETCHY’ WEBSITES

You should assume that any activity you are doing on a work device is being monitored and is accessible by your boss. Companies often have cybersecurity measures in place like DNS filtering that is designed to protect against phishing websites.

This same type of software can also send an alert should an employee be frequenting a sketchy website deemed dangerous to security (which many sketchy websites are).

As a rule, you should never visit any website on your work computer that you wouldn’t be comfortable visiting with your boss looking over your shoulder.

4. NEVER ALLOW FRIENDS OR FAMILY TO USE YOUR PC

When you use a company laptop or your work computer is a permanent fixture in your home, it can be tempting to allow a friend or family member to use it if asked.

But allowing anyone else to use your work computer could constitute a compliance breach of data protection regulations that your company needs to adhere to.

Just the fact that the personal data of your customers or other employees could be accessed by someone not authorised to do so, can mean a stiff penalty.

And there's always a risk that someone who is not well-versed in cybersecurity could end up visiting a phishing site and infecting* your work device, which in turn infects your company cloud storage, leaving you responsible for a breach.

**According to Malwarebytes, at least 20% of companies have experienced a data breach during the pandemic due to a remote worker.*

5. NEVER TURN OFF COMPANY-INSTALLED APPS LIKE BACKUPS AND ANTIVIRUS

It’s frustrating when you’re trying to get work done and a backup kicks in, slowing your PC down to a crawl.

It can be very tempting to turn off the backup process, but this can leave the data on your computer unprotected and unrecoverable in the case of a hard drive crash or ransomware infection.

Company-installed apps are there for a reason and it’s usually for cybersecurity and business continuity. These should not be turned off unless given express permission by your supervisor or company’s IT team

SUMMARY

It’s easy to slip into bad habits.

Using your work computer for personal tasks is a very common one.

Try and break the habit and think twice before you do any of the following,

1. Save your personal passwords in the browser
2. Store personal data
3. Visit sketchy websites
4. Allow friends or family to use it
5. Turn off company-installed apps like backups and antivirus

Check your company IT policies and remember that these policies protect the company but there also there to protect you.

ABOUT US

We're Trusted Computing, a small dedicated team based in the North West of England..

We help small, growing businesses in Greater Manchester and Cheshire take those difficult first steps towards using and trusting an external provider to manage their IT.

Our aim is to keep things simple. We focus on what we do best, so that you can do the same.

https://trustedcomputing.ltd/about-us/