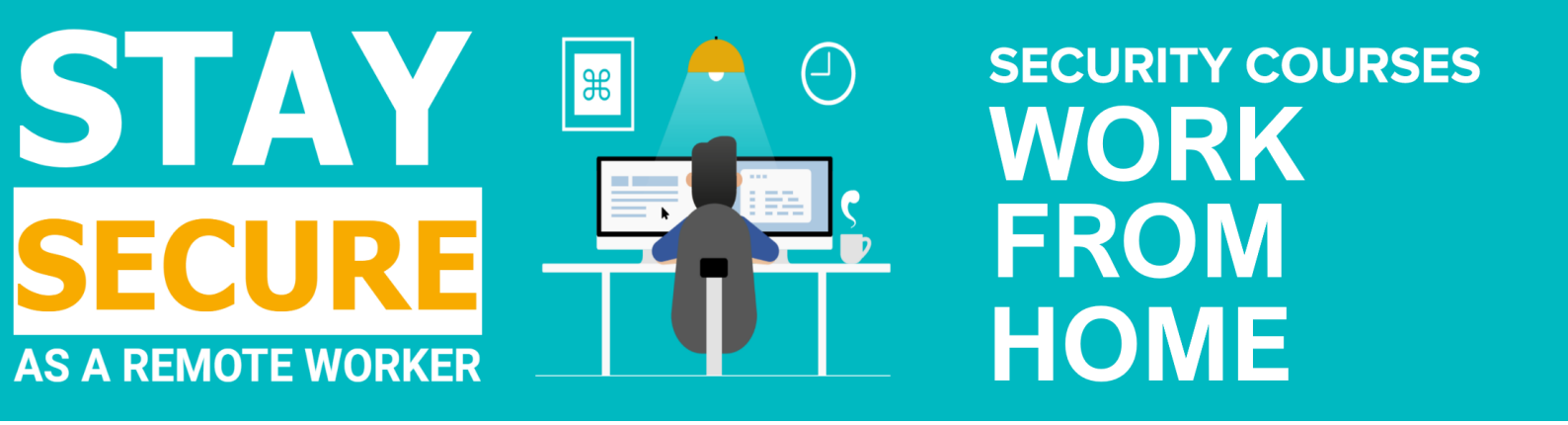


REMOTE WORK SECURITY COURSE

There are many benefits to working at home or away from your office. These Include less time commuting, less office distractions and a lower chance of catching a serious infection. Whether you work from home or at another place across the globe, YOU are responsible for ensuring the security of your person, your devices, and any data you carry.

You can't rely on the high level of security at the office. So, you need to prepare well for working away from your office. If you don't, you risk being an easy target for thieves, pick-pockets, unscrupulous competitors, and other criminals. These criminals want to steal your personal or employer's data. Good preparation can reduce your risks and make your remote work experience better and safer.

WHAT SECURITY RISKS DO YOU FACE WHEN WORKING REMOTELY?

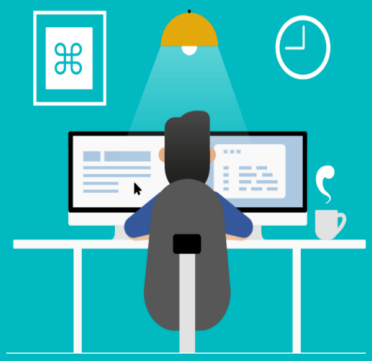
Many things can reduce the security of remote workers and the company data you use daily.

In this course, we have grouped these risks into four major categories. Physical theft or loss. Lack of personal awareness. Unsecured public connectivity, and unrestricted organizational access.

PHYSICAL THEFT OR LOSS

Working in an office gives you many support systems. These systems include extra security and people. You get Data Security systems, good security practices and Security Officers.

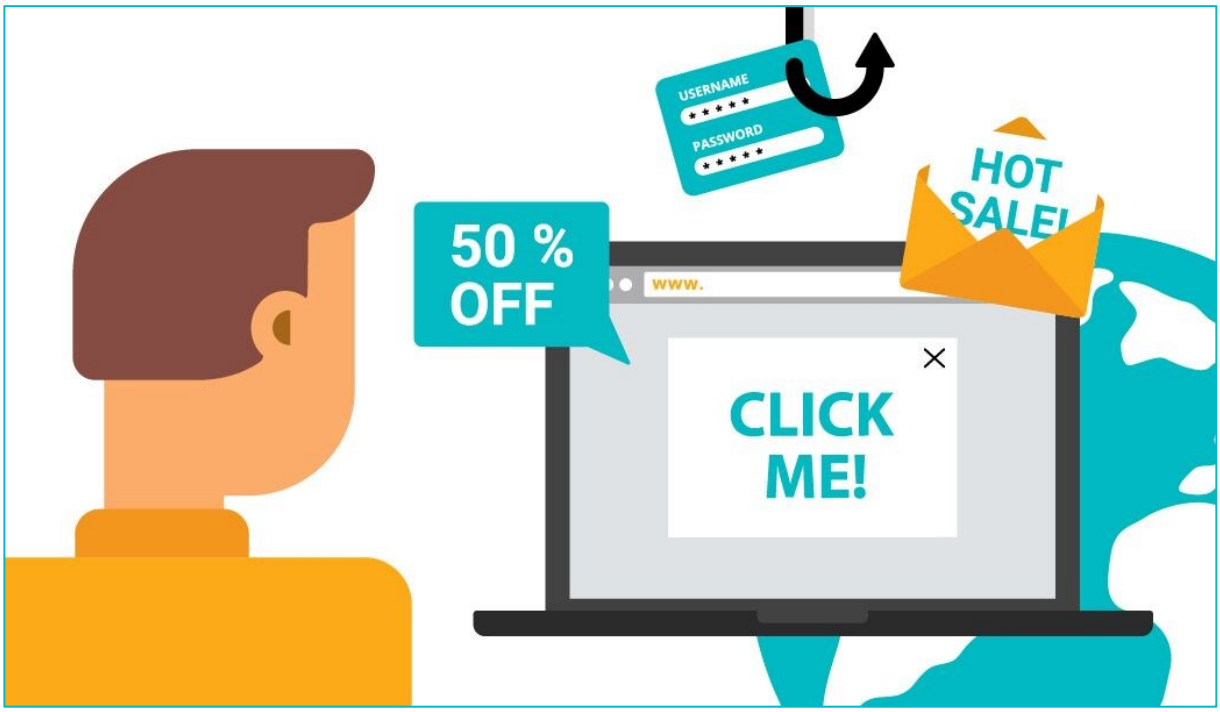
STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

LACK OF PERSONAL AWARENESS

In many cases, working at home brings less distractions. If you are well organized you can focus more when away from the office environment. Without the habit of constant vigilance, you may not notice that you are a target.

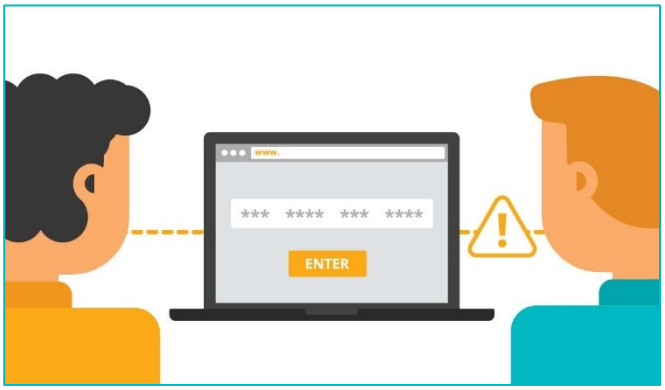


You may be accessing your employer's data using your personal or a public device. Or worse, are browsing the web from an officially issued device. Either practice can compromise your security and the data of your employer.

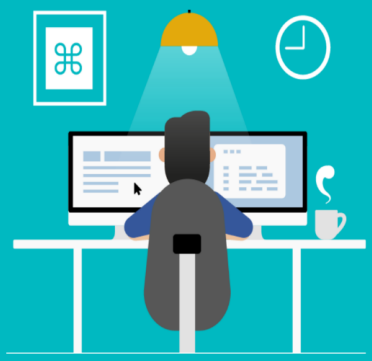
UNRESTRICTED COMPANY ACCESS

Many organizations give remote workers the same access rights that they would have in a safe office. This includes full access to all networks, cloud storage, internal systems, etc.

If you are not diligent or you lack security awareness, such privileges can give an attacker full access to your employer's data.



STAY SECURE AS A REMOTE WORKER

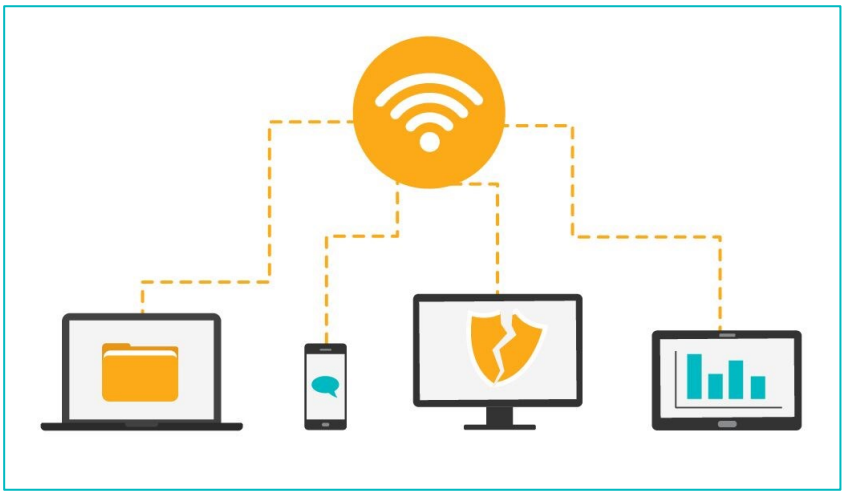


SECURITY COURSES

WORK FROM HOME

UNSECURED PUBLIC CONNECTIONS

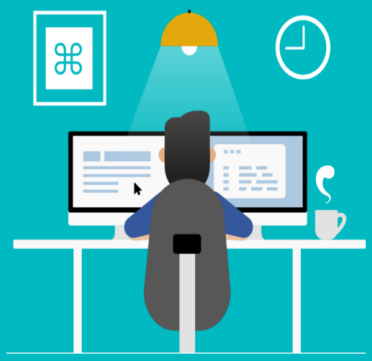
How many times have you used a public Wi-Fi network when traveling? In a coffee shop, at the airport or a hotel room?



Most of these networks have no security. Which means that using one for your work needs exposes your device and data to potential hacking.

The threat is real because most public networks aren't encrypted. The network does not ask you to authenticate to connect. Such networks can grant hackers access to all of the information you are sending on the Internet. From confidential emails, to your company's security credentials, and even credit card details.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

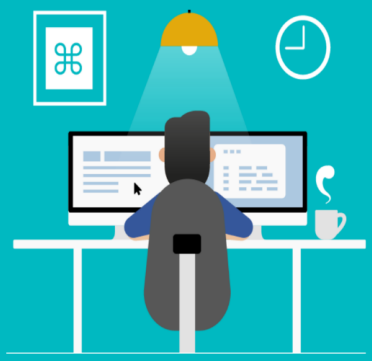
WHAT CAN YOU DO TO PROTECT YOURSELF AND YOUR EMPLOYER WHEN WORKING AWAY FROM THE OFFICE?

Good news! Anyone can secure their remote office. You will need to develop good habits. Stay aware of security procedures at all times.

STEP 1: PREPARE YOURSELF AND YOUR MATERIALS

When you need to work away from the office, whether you're traveling or just working from home, be sure that you are prepared to perform your tasks securely. The I.T. support team will give you advice. They will show you how get secure remote access to files and systems that you will need to do your work.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

Before you leave to work from home pack your computer and any documents that you will need in your line of work. Don't take everything. Leave customer confidential data, business plans, protected information, and proprietary data at the office. This precaution will reduce the number of things you must keep secure. If a thief steals your device or you lose it you will have reduced the impact to you and your employer.

STEP 2: KEEP YOUR DEVICES UP-TO-DATE AND SECURE

To secure your devices, you have to make sure all installed software, including the operating system, is up-to-date. Keep in mind that no operating system is completely secure. Security companies and Hackers find weaknesses all of the time affecting any version of your software. The risk is much higher when the operating system is older and unsupported. It is best practise to make sure your devices always run on the latest supported OS version.

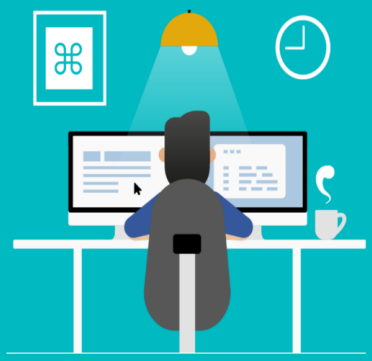
Most security vulnerabilities take over two months to resolve. Imagine what can happen to a system if it's exposed to threats for that period of time? Eliminate the delays in updating your device with the latest security patches: turn on the automatic updates option. Allowing your system to download and apply these updates as soon as they are available is always best advice.

Once your system is secure with regular updates, it is time to turn your attention to all the other programs that run on it. Office or creative suite, browser and any other software that can make you vulnerable. Most software checks for updates, so all you need to do is switch on automatic download updates.

STEP 3: LOCK YOUR COMPUTER WHEN STEPPING AWAY

When you're working away from the office, you must make sure your officially-issued computer is secure. Both the laptop itself and the information it stores. These are valuable to a thief or a competitor. Take these precautions to ensure the safety of your device and all of the data it contains:

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

✓ STEP 3.1: ENABLE DEVICE LOCKING

Any time you walk away from your device, make sure you lock it. In case you forget to do it, set up your device to lock automatically. Set it to lock when inactive for 30 seconds for a phone/tablet or 5 minutes for a laptop.

✓ STEP 3.2: TURN OFF AUTOMATIC LOGIN

No one but you should be able to access your device. So, make sure that logging in requires authentication. Use a strong password, pin, or a biometric alternative. Automatic logins are a real threat to your employer's security. So, make sure you switch this off at all times.

✓ STEP 3.3: USE STRONG PASSWORDS

We can't stress enough the importance of using strong passwords and pins on all of your devices.

Weak passwords include same or consecutive letters/numbers. Easy guessed common words, and personal information that is available on social media. (Such as birthplace, birth date, license plate, etc.).

A strong password looks random to others. It should include at least 8 characters of mixed lower- and uppercase letters, numbers, and symbols.

✓ STEP 3.4: INVEST IN A PASSWORD MANAGER (MANY ARE FREE)

When you use strong, unique passwords for all your devices and accounts, it gets difficult to manage them. You may forget a password and you should not keep them on a sheet of paper. This is where a password manager comes in. They can store a lot of information, encrypt it, and wrap it up in a single password that you can keep track of. Options include 1Password, LastPass, and many others.

✓ STEP 3.5: USE TWO-FACTOR AUTHENTICATION (2FA)

In many cases, having just a password to protect your accounts is not enough. Especially when logging in to IT systems, online banking, emails, or your password manager. All of these places hold significant, high-value data which you must keep safe and secure at all times.

What is two-factor authentication (2FA)? It is a system that you need a password and an additional verification method to prove your identity. This could be a one-time code sent via SMS or could go through an authenticator app. Having 2FA enabled on all your devices and accounts will make you breathe easier.

✓ STEP 3.6: ENABLE “FIND MY DEVICE” AND “REMOTE WIPE” OPTIONS

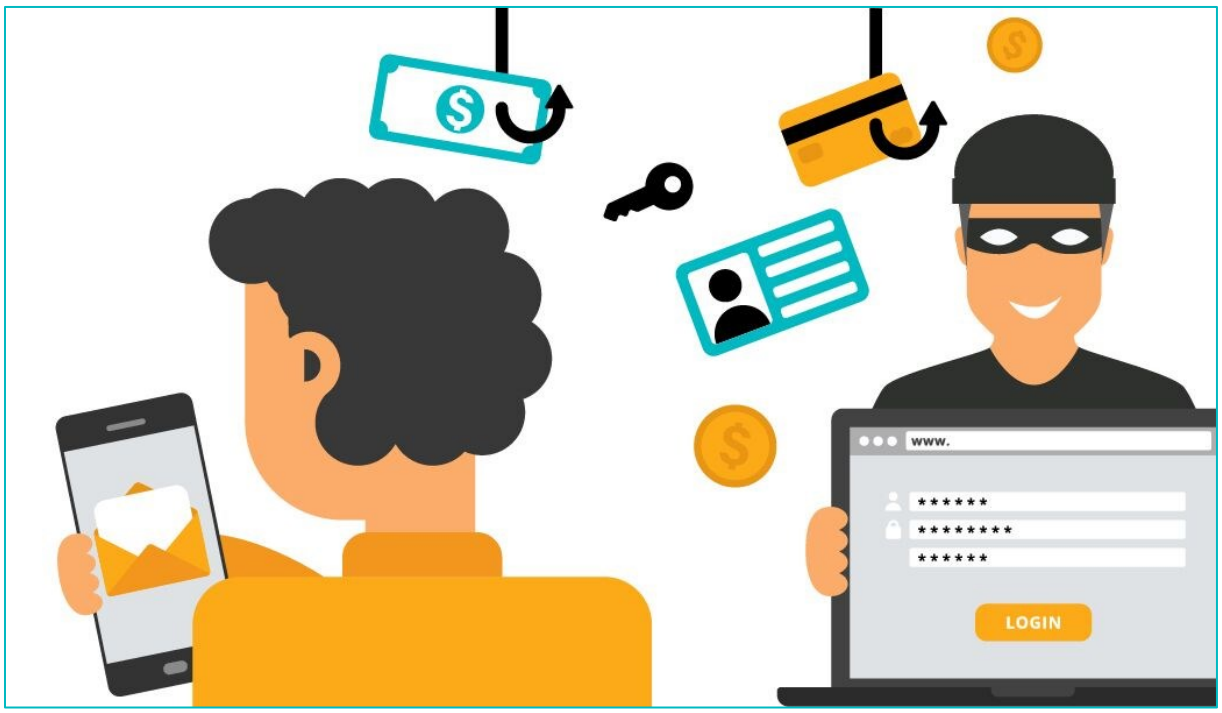
In cases of loss or theft of your device, having the option to remotely locate and wipe the contents of your device is critical. Wiping can save your data, both personal and corporate, from falling into the hands of attackers.

✓ STEP 3.7: FACTORY RESET

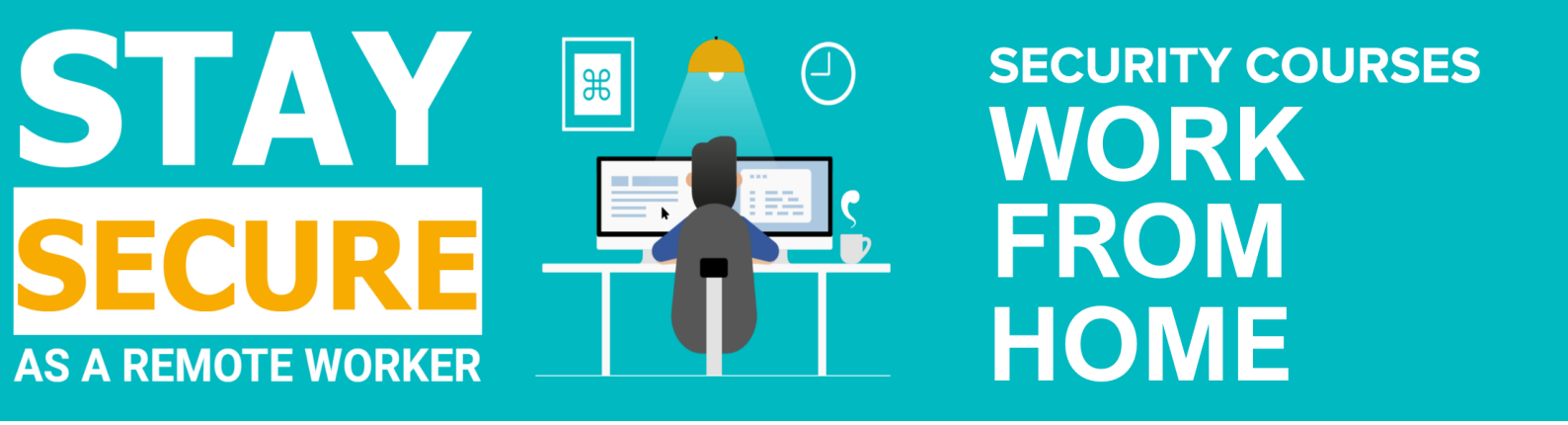
You should always Factory reset your devices when no longer needed. Reset the device to factory settings before selling, giving, or otherwise disposing of it.

Remember that wiping deletes all information stored on the device. If you need this information for future use, make sure you back it up first!

STEP 4: BE AWARE OF YOUR PHYSICAL SURROUNDINGS



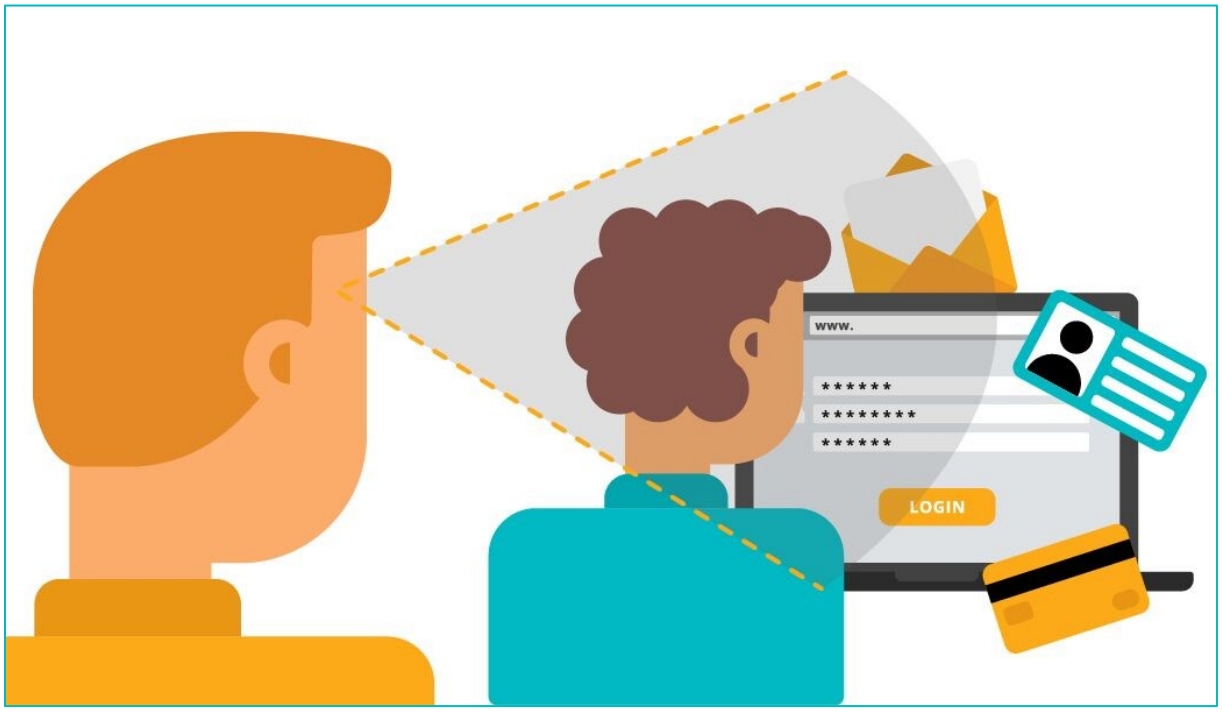
Your physical surroundings are so important. Neglecting them can compromise the security of your person, your device, and your employer’s data. This is especially true when working at home. Always close and lock your doors.



Stay vigilant of activities occurring around you. Never leave any device or thumb drive unattended in public places. In the time it takes you to use the restroom, a thief could steal your laptop. A criminal can infect your machine with malware. Loss of your device and information stored on it can cause stress and disrupt your work process. Lost data can result in fines for you and your employer.

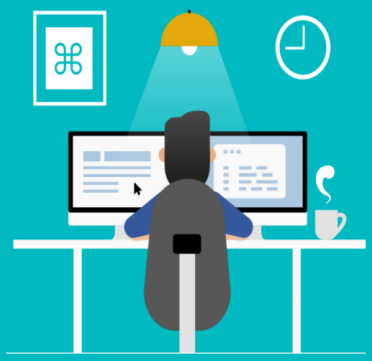
When working from a public location, pay attention to your sight lines. If possible, sit with your back to a wall so no one can look into your screen from behind (also known as shoulder surfing). Another option is installing a privacy filter. The filter stops anyone but you looking at your screen.

STEP 5: PAY ATTENTION TO YOUR SIGHT LINES



When working from a public location, pay attention to your sight lines. If possible, sit with your back to a wall so no one can look into your screen from behind (also known as shoulder surfing). Another option is installing a privacy filter app, which doesn't allow anyone looking at your screen at an angle to snoop for information they're not meant to see.

STAY SECURE AS A REMOTE WORKER



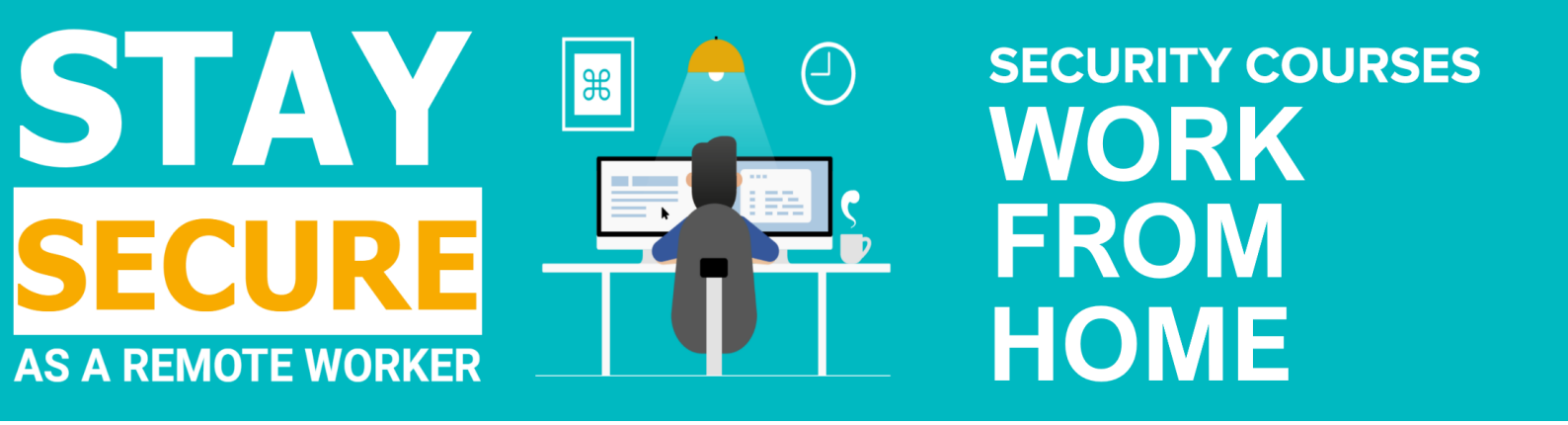
SECURITY COURSES WORK FROM HOME

STEP 6: PROTECT CONFIDENTIAL INFORMATION

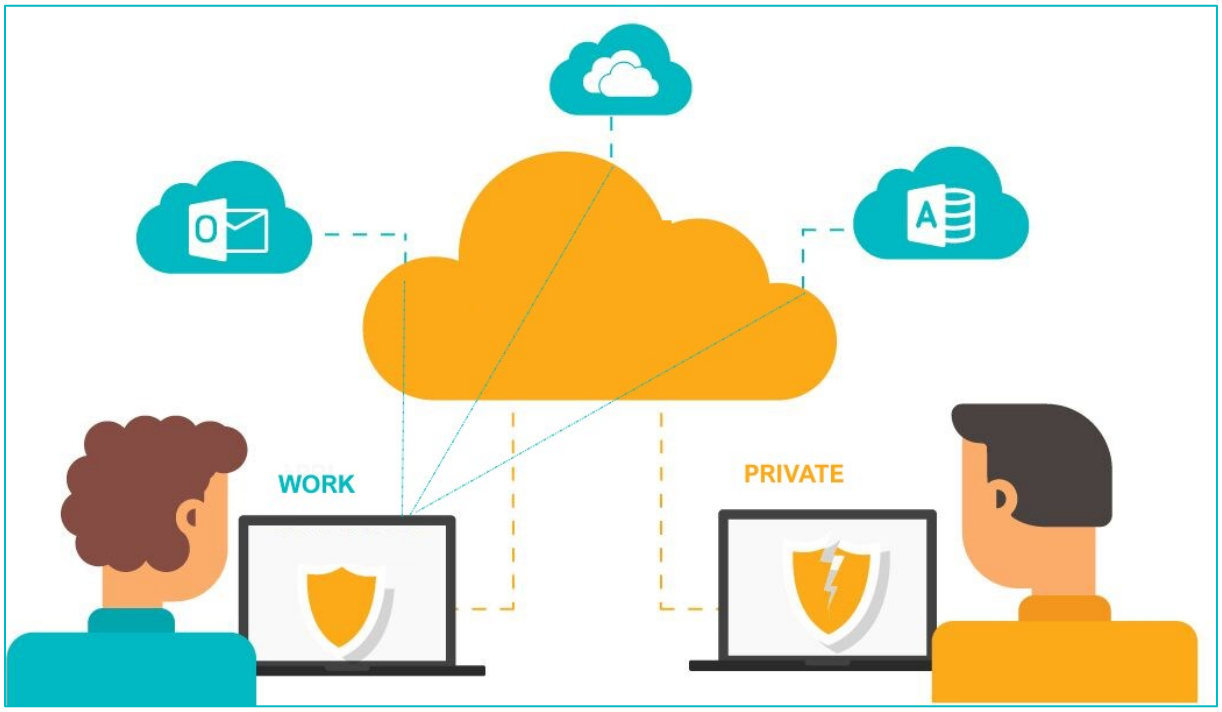
When working away from the office, protect any confidential or personal information that you use, carry, and store. In a public setting, many people could have malicious intent. If you lose personal information your company may be held liable for disclosing protected information.

Public computers aren't safe. You should never use them when personal or confidential data is involved. You don't know that malicious software hasn't been previously installed on a public machine. So, avoid entering any confidential information. This includes login credentials, bank account information, social security numbers. If you must use a public computer, make sure you use “private browsing. Do not check any “save” or “remember” boxes. Clear your browsing history and delete all downloads before closing the browser.

Do you travel with your office computer or work on it at home? There is still a danger if other people have access to it. Keep your officially-issued devices for work only. Don't allow anyone to use them, including friends or family. Even unintentional compromise of confidential data can still make you liable for its loss.



STEP 7: KEEP WORK DATA ON WORK COMPUTERS

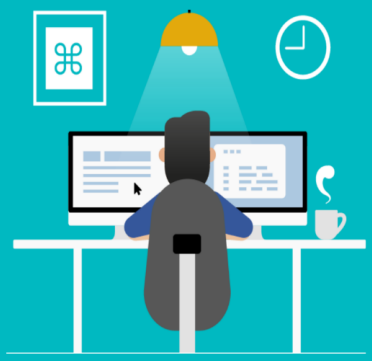


It is likely that your personal devices are not frequently updated, are not scanned and don't constantly run finely-tuned antivirus. They do not sit behind a firewall with encryption on a private network. If you're not an IT specialist yourself (and even that's not a 100% guarantee!) you're likely unfamiliar with all the precautions that an efficient IT teams makes at corporate level.

You may want to use your work computer for personal things, such as online shopping, banking, or even checking your email. You may want to use your personal devices for work tasks. Connecting any device to your corporate networks is dangerous. It can jeopardise the safety of your entire work system, making you liable for any damage to or loss of confidential data stored on company servers.

You can eliminate risk if you need to work from your personal computer. You can use cloud-based environments such as Office 365. Via these services, you work online without downloading or synching files or emails to your personal device.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

STEP 8: AVOID PUBLIC WI-FI

When you're working from a public location, it's very tempting to use the available free public Wi-Fi. But the security risks that 'easy' access can cause are great. They will very likely lead to trouble for you and your employer.

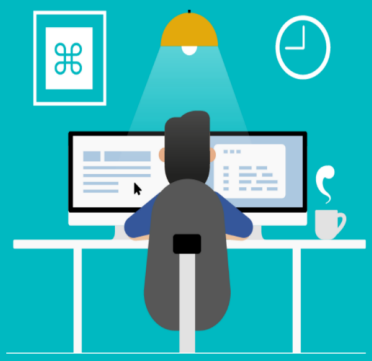
The two problems that public Wi-Fi cause are:
1) Unprotected network shared by many devices at once.
2) Unprotected data traffic that goes between the public Wi-Fi you're using and the network at your workplace.

To resolve the first part of this problem, you can opt to set up your own personal Wi-Fi network. This is a hotspot. It uses your phone or other mobile device to connect. A hotspot doesn't encrypt your traffic, but it doesn't allow anyone on the same network to capture your data. You may be charged by your carrier for setting up your own private Wi-Fi network. But the fee will be nominal compared to the potential damage of using public wireless networks.

To work around the second issue, a good solution is setting up a VPN. A VPN is a Virtual Private Network. It provides a secure and encrypted channel for your traffic as it travels through the Internet. A VPN makes it extremely difficult for cybercriminals to intercept your data. It hides your real location and gives you the online privacy you need.

Some countries ban the use of VPNs. If a VPN is legal where you are, it's a good practice to set one up when working from public locations.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES

WORK FROM HOME

STEP 9: ENCRYPT SENSITIVE DATA IN EMAILS AND ON YOUR DEVICE

No information sent via email is secure unless you make certain to encrypt it first. Encryption is a process that encodes the information. It does this in a way that makes it difficult to open by unauthorised parties. If you need to send sensitive data over email, make sure that you encrypt it first.

As a precaution, you should always encrypt all of your stored data. Do this so that if your device is lost or stolen, no access to the stored information is possible without your password or pin.

STEP 10: BE CAUTIONS OF USB DRIVES AND PORTS

Would you be pick up an abandoned flash drive and plug it into your computer? Don't! This is a classic hacking method but many people still do it.

If a USB stick gains access to the data ports of your computer, your data and your entire corporate network can be compromised. Never plug in an abandoned USB drive.

A dangerous practice is plugging in your device to charge via USB at a public phone charging station. If this is your only charging option, you must use a USB Data Blocker. The Data Blocker connects the power leads of the port only and doesn't use the data ones.

STEP 11: NEVER LEAVE WORK COMPUTERS OR DEVICES IN A VEHICLE, HOTEL ROOM, OR OTHER UNSECURED LOCATION

To avoid theft of your work devices and sensitive personal or corporate data, always keep them on your person when you're working remotely. Don't leave them in your car, not even in the trunk. Hotel rooms aren't safe either, as hotel staff can access them at any time.