Interreg
Baltic Sea Region
Co-funded by
the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Cyber Security in Remote Work: Safeguarding Your Data

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

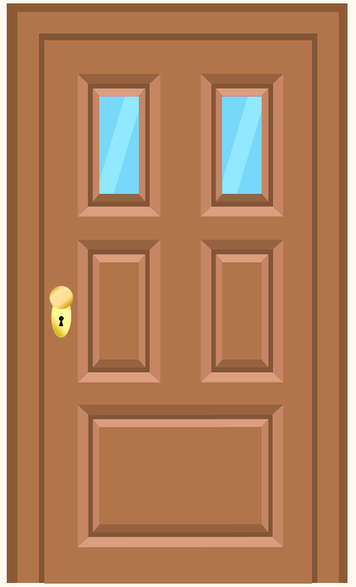
In this new era of remote work, cyber security is not an option, it's a necessity.

Follow these rules for working from anywhere:

Watch Out for Tricky Messages: Sometimes, bad guys send messages that look real but are trying to trick us. Be careful with emails or messages that seem odd or ask for personal information. It's like being cautious about strange letters in your mailbox.

When working from multiple places and devices, there are more ways for bad guys to try and get into our systems. It's like having more doors and windows at home – we need to make sure they are all locked and secure.

Just like at the office, there are rules for how we should work from multiple places. These rules help keep our work safe and sound. It is like having guidelines for how to handle important papers.



Learn the Basics of Cybersecurity

Just like when we learn to look both ways before crossing the street, it's important to learn to keep our work safe online. Continuous training helps us stay aware and avoid digital dangers.

Have a Plan for Emergencies: What if something goes wrong? Having a plan is like having a superhero team ready to fix things if there's trouble. Also practice the plan so everyone knows what to do, just like when you practice with a fire drill.

With the right precautions, we can make sure everything stays protected.

Understanding Cyber Threats

Secure your remote work environment by
-using strong passwords,
-two-factor authentication,
-a reliable VPN.

Also backup your data regularly.

Safe Remote Work Practices

Use strong passwords and enable two-factor authentication.

A good password exhibits the following features:

Length: Use at least 12 characters. The longer the password, the more difficult it is to crack.

Complexity: Mix uppercase and lowercase letters, numbers, and special characters. This adds complexity and makes the password harder to guess.

Avoid easily guessable information: Refrain from using easily obtainable information, such as birthdays or names.

Avoid common words: Steer clear of common words that can be found in dictionaries or easily guessed.

Use different passwords for different services: Do not use the same password across multiple accounts. If one password is compromised, the security of other accounts remains intact.

Regularly update your passwords: Change your passwords periodically to ensure that even if a password is compromised, it won't be valid for an extended period.

Use password management tools: Consider using password management tools to store strong, unique passwords for each service.

A passphrase can be used instead of a password, and it can provide additional security in cybersecurity:

Length and complexity: Passphrases can be long and complex, making them more challenging to crack compared to shorter, traditional passwords.

Ease to memorize: Sentences are often easier to remember than random character strings.

Natural feel: A passphrase, which resembles a sentence, may feel more natural and user-friendly compared to random character strings. This may encourage users to choose stronger and more unique passphrases.

Less susceptible to dictionary attacks: Traditional short passwords are more susceptible to dictionary attacks, where an attacker rapidly tests a large number of words. It is harder to find a passphrase in a dictionary, especially if it includes unusual words or combinations.

Combined complexity: A passphrase can effectively combine uppercase and lowercase letters, numbers, and special characters, enhancing overall complexity.

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Multifactor Authentication is like having multiple locks on the door to your online accounts.

Multifactor Authentication (MFA), sometimes also called Two-Factor Authentication (2FA) adds an extra layer of security. This makes sure that only you can access your accounts, even if someone else knows your password.

Enable Multifactor Authentication wherever possible.

This adds an extra layer of security by requiring users to provide a second form of authentication, such as
-a one-time code sent to their mobile device or
-a fingerprint scan.

Multifactor Authentication MFA - How it works?

The first lock (your password): Think of your password as the first lock on your online account. It's like a secret code that you use to prove you're you when you want to log in.

The second lock (something you have): MFA adds a second lock, which is something physical that only you have. This could be your smartphone, a special app, or a hardware token (like a small device). It's like a key that goes with your password.

How it works: When you log in, you'll enter your password, which is the first lock. But with MFA, you also need to provide something from the second lock. For example, you might get a code on your smartphone, and you have to enter that code.

Why it's important: MFA is like having an extra layer of protection. It makes it much harder for online criminals to break into your accounts even if they somehow figure out your password. It's an extra safeguard for your online security.

Secure Network Connection

Working remotely requires a secure network connection to protect sensitive data from cyber attacks.

Avoid using public Wi-Fi for confidential work activities.

Use VPN.

VPN - Virtual Private Network

A VPN is like a secure tunnel for your internet connection. This is a way to protect your online activities and keep your data safe.

When you connect to the internet without a VPN, it's a bit like shouting your questions and answers in a crowded room. Everyone can hear you, and some people might try to listen in on your conversations.

When you use a VPN, it's like having a private conversation in a soundproof room. Your questions and answers are still there, but they're hidden from prying ears. A VPN creates this private, secure space for your internet activities.

Why would you use a VPN?

Privacy: It keeps your online activities private. Nobody can eavesdrop on what you're doing, not even your internet service provider.

Security: It adds a layer of security, especially when you're on public Wi-Fi networks. This makes it harder for hackers to steal your data.

Access: A VPN can let you access websites and content that might be blocked or restricted in your location.

Anonymity: It can also help protect your identity by masking your real IP address. This can be important for people who want to stay anonymous online.

Think of a VPN as your online bodyguard, ensuring that your internet activities are safe and your personal information is kept private.

Secure Devices and Software

Keep your software and antivirus up-to-date to stay safe from cyber threats.

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Regular software updates are like getting your car serviced to keep it running smoothly.

Software updates play a crucial role in preventing cyberattacks

New features and fixes: Just like cars, computer software needs maintenance and improvements. Software developers regularly release updates to add new features, fix problems, and make everything work better.

Security patches: Think of these updates like installing strong locks on your doors and windows. They help protect your computer from bad guys who might try to break in. When you update your software, you're adding these new locks.

Better performance: Software updates can also make your computer run faster and more efficiently, just like a well-maintained car runs better.

Compatibility: Sometimes, new software updates ensure that your programs and apps work well together, like having the right kind of fuel in your car's engine.

When your computer or phone tells you it's time for an update, it's like a reminder to take your car in for a tune-up.

Backups

Remember to make copies of all important information.

Backups are insurance – they make sure your important information is safe and sound, even if your computer malfunctions.

What are backups?

Backups are like safety nets for your digital data. They're copies of all the important information on your computer or device – like pictures, documents, and even the settings that make your computer work just the way you like it.

Why are backups important?

Imagine if your computer suddenly stopped working or you accidentally deleted something important. You could lose all your favorite photos or important work documents. Backups are like having a spare set of keys – if you lose one, you can always use the other to get back in.

How to backup?

Backing up is usually pretty easy. You can use special programs or even built-in tools on your computer. Some people also like using external hard drives or cloud services (like a digital storage locker) to keep their backups safe.

Interreg Baltic Sea Region
Co-funded by the European Union
RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Here are a few reasons why backups are crucial:

Accidents happen: Sometimes we click the wrong button or something just goes wonky. With backups, you can easily go back to how things were before the accident.

Computer malfunctions or crashes: Computers are smart, but they can get confused or tired. If your computer ever decides to take a nap, you won't lose your data if you have backups.

Protects against viruses and cyber criminals: Viruses or cyber bad guys can try to mess up your computer. With backups you can get everything back to normal.

New devices or upgrades: If you ever get a new computer or upgrade your existing one, backups make it super easy to transfer all your data to the new device.

Interreg Baltic Sea Region

Co-funded by the European Union

RESILIENT ECONOMIES AND COMMUNITIES
Distance LAB

Stay safe and secure online!

https://interreg-baltic.eu/project/distancelab/

Interreg
Baltic Sea Region

Co-funded by
the European Union

RESILIENT ECONOMIES AND COMMUNITIES

Distance LAB