CyberMSME

Cybersecurity for Micro, Small & Medium Enterprises

Improve your cybersecurity management plan – best practices

By CTS Customized Training Solutions & CASE

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of contents — click to skip to the relevant page:

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

You can improve your cybersecurity management plan staring with the following steps:

1. Enforce passwords

It seems obvious that a strong password is the first line of defense against breaches. Changing passwords from time to time helps hackers to break them.

Passwords best practices

You might have heard that the best password contains at least 1 capital letter, at least 1 number, and at least 1 symbol (like % # &). It has to be greater than 7 characters. Just take a look at an example.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Let say that your dog's name is Rusty. You adopted him in 2018. So the password on your laptop, the business cloud, and work e-mail is **Rusty-2018**. Easy to remember, right?

Also, easy to crack.

So, what to do?

Learn how to create strong passwords. A good, hard-to-crack password have to be:

- **long (not shorter than 15 characters)**
- **mixed of lower and upper characters**
- **free of common substitutions (e.g. "h0m3" instead of "home" is too obvious)**
- **free of common using keyboard paths (like "qwerty", "12345")**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Use passwords managers

A password manager is a computer program, web-based service, or plug-in that allows users to generate and manage their passwords. You can choose Keeper, LastPass, or DashLane.

If you can't choose one, you can read more about various passwords managers and their specifications following this link:
https://en.wikipedia.org/wiki/List_of_password_managers

2. Instead of using passwords, use passphrases

A **passphrase** is a combination of words and symbols that form a sentence. A sentence doesn't have to be grammatically correct. Passphrases usually contain up to 40 characters. The difference is noticeable in spaces — passwords don't have them, passphrases do have.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Passphrases best practices

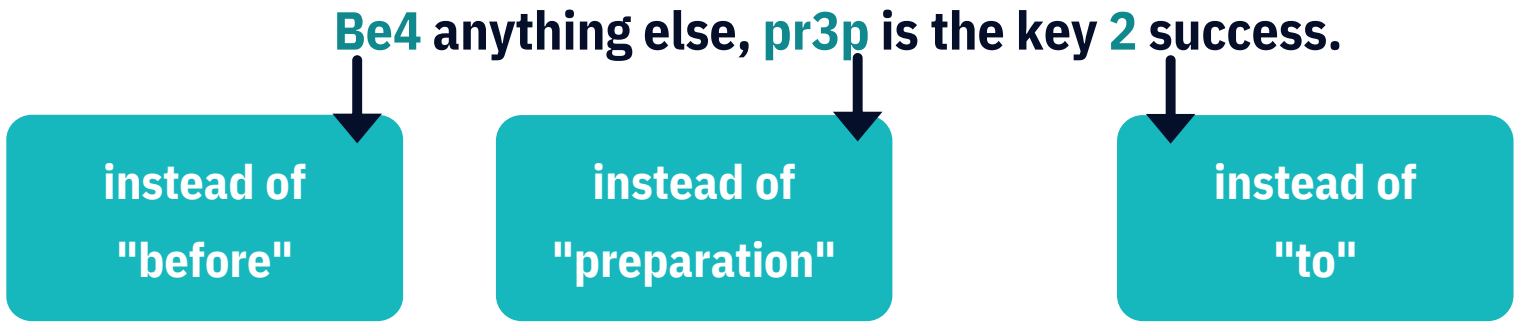
- Use an easy-to-remember but uncommon phrase.
- Use uncommon and/or abbreviated words.
- Add spaces.
- Use capital letters (at the beginning of the sentence or for chosen words).
- Change some letters with numbers.
- Add punctuation

Relevant links: TechTarget > Passphrase (https://searchsecurity.techtarget.com/definition/passphrase);
John Carroll University > Password vs Passphrase (https://password.jcu.edu/public/passphrase.php)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

A passphrase may look like Alexander Graham Bell's quote:



Or like random words and numbers:

Male h0rse 21, viLLag3 rAce.

Whatever you choose, remember to change your passwords regularly. Do not write them down anywhere where somebody else can acquire access to them. Decide who should know them — not everyone in your team must get to know each password and passphrase.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cyber MSME

3. Wherever possible, use more than 1 layer of authentication

A hacker may crack even a strong password or passphrase. That is why wherever you have this possibility, use **Two-Factor Authentication (2FA)**. 2FA is an additional layer of security for your password/ passphrase created to guarantee that nobody except you can access your account, even if someone else knows your password.

How does 2FA work?

- You may find 2FA using many apps and web services. In the first step, you use your login and passwords/ passphrase as usual.
- In the next step, the app/ website sends you a temporary verification code (e.g. on your mobile number). You need to enter the code in the app/ website to log in.
- Another possibility of the 2FA is a biometric-like fingerprint or face scan.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Never text or e-mail anyone your password

In case you need to share some passwords or passphrases with your employees, use a password manager like Keeper, LastPass, or DashLane.

5. Select hard-to-guess security questions

While creating an account you often need to select a security question in case you forget a password. Most of those questions have easy-to-find answers in your social media channels (e.g. your favorite movie, date of the first date, name of the first cat, etc.).

Be aware of that and choose your questions carefully. Also, teach that your employees and partners.

Relevant link: Avast > How to create a strong password (https://blog.avast.com/strong-password-ideas)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. Update regularly all apps

Make sure that your antivirus software is regularly updated. Scan your computer at least once a week. Remember that any connection to the Internet may be vulnerable and you probably use it every day for hours.

Also, care about updating your operating system, web browser, cloud, communication apps, etc. The smallest vulnerability can make it easier for hackers to exploit your business.

7. Update regularly your devices

Entrepreneurs often forget about updating devices different than laptops or smartphones. Yet all businesses possess more things that can be targeted by hackers. An attacker may hack your router, printer, or fax machine. Make sure your firmware is up to date on all devices having wifi connection — even microwave and oven in your kitchen.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

8. Be careful when using public wifi

Public wifi is available almost everywhere, with access points ready to use in restaurants, coffee shops, or airports. As an entrepreneur, you may need internet access in various places. The question is: are you safe using public WiFi?

Whenever it is possible, try to use your own internet provider. You can make your phone a mobile hotspot or buy a dedicated device. That is always safer than public wifi, which due to accessibility may be prone to hackers sniffing on sensitive data

What can protect you and your business while using public WiFi?

The best and most accessible option is to use a VPN to protect your privacy.

Relevant link: Kaspersky > **Public Wifi Security** (https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

What is VPN?

VPN stands for **Virtual Private Network**. Virtual means that the network is not really existing in a physical way, but is made by software instead. Private is self-explanatory: it is a network, that cannot be reached freely on the Internet. It is generally much more secure than a public network because it restricts connections and data cannot be easily spied on by hackers preying on a public network.

How to get VPN access?

You can set up your own VPN or use one of many paid VPN service providers. Be cautious! While you may stumble upon free VPNs around the web, using them might be even more dangerous than using the free wifi at the airport. It all comes down to how the VPNs work.

Relevant link: Algo VPN > **Self hosted VPN solution** (https://github.com/trailofbits/algo)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

How does a VPN work?

When you access any resource on the Internet, the whole communication is happening via packets. To put it simply, a packet is a small chunk of data passed over different routes to reach the end destination. Here is how a simplified "life" of a packet looks like without VPN:

Notice how your packets travel unencrypted through the free wifi network. Any hacker that gained access to the free wifi network may intercept and thus steal any sensitive data you send/receive.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Now let's compare that to the "life" of packet with VPN enabled:

As you can see, the packet is encrypted all the way to the VPN server. How does it happen? The VPN client installed on your device encapsulates the original packet in another, encrypted one. That encrypted packet then gets sent through the free wifi and the Internet Service Provider to the VPN server. Finally, the VPN server decrypts the original packet and passes it to the original destination. Comparing that to the previous example, even if the hackers will get a hold of the encrypted packets on the free network, they still would need to crack the encryption first to see your data.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Drawbacks of using VPNs

Of course, as with everything, there are drawbacks that come with using VPNs. First of all, the VPN you are using must be absolutely trustworthy. While there might be someone trying to intercept your data on a public network, the VPN you are using will by design intercept all of your data. That means that VPNs set with malicious purposes in mind are extremely dangerous to your business.

Second of all, the popular VPN providers, due to the security they provide, often attract bad actor users. You might find yourself being banned from accessing popular sites or resources due to sharing the same end IP address with someone that used it for a bad purpose in the past.

Lastly, the speed. The extra layer of protection usually limits the speed at which you can access your resources. While this is negligible when using free wifi networks (where the Internet speed is not very high, to begin with) it might limit your home network performance.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

9. Create an inventory list

Nowadays, owning a business requires much more from you and your employees than just a few years ago. You need to remember multiple names of apps, logins, passwords, etc. What if someone forgot its credentials? What if one of your employees lost his/ her smartphone? What should you do?

First of all, prepare your business for all possibilities by creating an inventory list. Your inventory list must include all data about your devices and online services.

You or your cyber security expert should prepare the inventory list and revise it regularly. In case of any incident, you always have all data needed to implement the cyber crisis management plan.

How to prepare an inventory list?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Sample inventory list

- **List of devices > model, memory, storage, operating system, IP, serial number** > current user (employee's name) > date of entry
- **Configurations settings to specify if the device is securely configured** > specification, date of update> date of entry
- **Network connections, network protections, and VPN** > provider, location, status, configuration > date of entry
- **Antivirus and other protection software** > provider, status, location, date of update, update version > date of entry

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **List of apps and software >** provider, update version > person/ devices authorized to access > date of entry
- **List of users' accounts, including dormant, shared, local, admin, etc.** > location, status> date of entry
- **Backup** > status > date of entry
- **List of vulnerabilities, gaps, and attacks** > location, status, response and recovery steps > date of entry

Relevant link: Verve Industrial > **What is OT/ICS Asset Inventory and Why is it the Foundation of a Cyber Security Program?** (https://verveindustrial.com/resources/blog/what-is-ot-ics-asset-inventory-and-why-is-it-the-foundation-of-a-cyber-security-program/)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Where to store the inventory list?

Big companies use special platforms like:

- **Otorio** (https://www.otorio.com)
- **Axonius** (https://www.axonius.com/platform)

They have a free demo available so you can test them yourself free of charge.

You can also check out a solution created by the global IT community:

- **CIS Controls** (https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/)

This tool is free and open source. It is constantly updated, and among its developers are companies, government agencies, institutions, and individuals from every part of the ecosystem (cyber analysts, vulnerability-finders, solution providers, users, consultants, policy-makers, executives, academia, auditors, etc.).

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

10. Deactivate all unused services

Thanks to the inventory list, you can manage unused services, products, and apps that will expire soon or already expired. Do you remember how many times you entered your business data, including your credit card number to activate an app? Exactly...

So, if you don't reactivate the account, that information will be available for the potential hacker.

11. Revise connections between devices

Not all company's devices need to talk to each other or the network. Revise all connections and decide which one is necessary or not.

If you manage a huge database or financial transactions maybe it would be better to do that on one specific computer that has no connection with other company's devices.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cyber MSME

12. Create data access levels

Then again, just as not all devices need to talk to each other, not all of your employees need to have access to all data, accounts, and documents. If you have already created the inventory list, you can control your devices and software. Now is time to create another document that will help you manage your cybersecurity — data access levels.

Access level is a set of permissions or restrictions provided to access data.

If you are a programmer you can simply code access levels in the app or website. However, not only programmers should think about creating access levels. Even if you don't have an IT background you may do that.

Where to start?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Data access levels principles

As we said, access levels are based on a set of permissions or restrictions. First of all, you need to categorize all data, including app and software, and you must prioritize them, e.g.

category A	the highest level of priority
category B	high level of priority
category C	medium level of priority
category D	low level of priority
category E	the lowest level of priority

importance

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

These levels are exemplary, of course. It is up to you to decide how many of them there will be. The most important thing is that you realize which employees should have access to the data and on what basis.

For example, sensitive data that you keep in your customer database might only be accessible to 2 people who work on it every day. In case of a crisis, they are joined by 2 other employees. This is how you implement one of the points of the cyber crisis management plan.

In effect, only a few people are privy to the data. Think how this makes crisis management easier — if the above-mentioned data is shared outside the company, it will be easy to locate the leak. You will have 4 people to check, their devices and their operating history. That is much easier than checking all employees, partners, and suppliers.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

You can create a data access levels list by yourself or ask a cybersecurity expert for support. Whatever you choose, remember to inform your employees what level they get. Train them on what those levels mean in everyday work and in the cyber crisis situation.

Also, keep in mind to update the list regularly, especially, whenever one of your employees changes positions, gets promoted or leaves the company. Updating this list may be one of the responsibilities of a cyber crisis response person(s). If you manage a bigger team, you can assign another person to this task.

It could be:

- a cybersecurity expert
- a cybersecurity consultant
- a cybersecurity analyst
- an IT system admin.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

13. Don't keep all your data in one place

We don't mean that you can't keep your data in one secure cloud. The point is that if some key data about your business, like customer data or financial data will cover one screen, you make it easy for an attacker to take a screenshot in a matter of seconds.

Such data can also be easily stolen by taking a screenshot with a smartphone. So rethink the policy of having smartphones on your company property. Perhaps not everyone needs them, perhaps not in all places.

Remember also that a screenshot of a desktop screen can be taken when you or any employee is working in a coffee shop, hotel lobby, train, or airport. Train your employees that even connecting via VPN does not fully protect them against data hacking. They always need to protect themselves.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

14. Use TPU screen protectors

As we said, even VPN can't protect your data in a public place. That is why we recommend you use special screen protectors made from TPU (thermoplastic polyurethane).

This material is chemically-enhanced plastic that features include scratch resistance, flexibility, oil and grease protection, and increased toughness. Why do we think you need this?

Because it is also used in making screen protectors with special properties. TPU prevents the contents of your screen from being viewed by anyone who looks at it from the side.

For others, your screen will just be black. There will be no way to take a picture of any data. You, on the other hand, will be able to do your work normally — everything will be seen normally.

Relevant link: Viola Pan > **Part Three: PET, TPU, or Tempered Glass – all you need to know to choose a screen protector** (https://www.linkedin.com/pulse/part-three-pet-tpu-tempered-glass-all-you-need-know-choose-viola-vmax/)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

15. Teach others

Keep in mind that cybersecurity is not a one-time activity. It's a long-term plan that should be implemented progressively and wisely. It requires the involvement of all employees, although not necessarily in the same manner. It depends on the company's cyber crisis management plan.

Don't forget that people are the weakest link in your cybersecurity system. Train your employees, keep them informed of changes, updates, and new methods of social engineering.

Are you ready to start?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Thank you for your attention!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.