Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Essential router security tips

Enhance your network security with few basic steps

By CTS Customized Training Solutions & CASE

Erasmus+

By following those simple tips you can make your small company network much safer:

1. Look at your router manufacture date

Your trustworthy router has been with you from the beginning of your company? Do you treat it like an honorary employee? We get that, we really do! But when the security of your business is at stake, there is no room for being sentimental.

There is no easy way to determine whether you should change your device or not. Experts recommend replacing your router every 2-3 years, with the absolute maximum being 5 years. You should immediately change your device if it only supports an encryption protocol that is known to have major security vulnerabilities (more information regarding that topic that will be covered later).

Erasmus+

2. Update the firmware

Buying a new router, setting up the basics and then never touching the administration panel ever again? We have all been there! But there is a good reason to check in from time to time. Routers, like any other device connected to the Internet receive constant firmware updates. While some of the devices do update automatically, some require administrator input to do so – if you just leave it be as it you may miss out on important security updates, that can be used by bad actors to gain access to your network!

3. Turn off Wi-Fi Protected Setup (WPS)

While visiting the administration panel, be sure to turn off WPS. What's WPS? It is a method of connecting a new device to the network by pressing a physical button on the router. It may seem handy (you don’t have to memorize the password!) but it is really dangerous to keep on. Why?

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.

WPS is the most **common way among hackers** to **gain unauthorized access** to **your** network. Many hacker tools rely solely on exploiting WPS as a method to breach your network security. **Turning it off is one of the easiest and most important steps to keep your network secure!**

4. Do not use WEP or WPA encryption protocols (unless you have to)

While setting up your Wi-Fi you are asked if you want your network password protected (you do) and if so, what encryption protocol do you want to use. This is the place most of us start to panic as we are bombarded by enigmatic shortcuts (WEP, WPA, WPA-PSK, WPA2-PSK, and *a bunch more*). Why there are so many? Which one to choose? Let us answer those questions!

To keep it simple: encryption protocols are a way to authorize only those connections that have the required key (in our case, the Wi-Fi password) and keep the others away. WEP was the first ratified

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

standard and its beginnings go as far as 1999. It got superseded by WPA (Wi-Fi Protected Access) in 2003, which was followed by WPA2 in 2004. Since 2018, WPA3 became available for use.

So which one should you use? The simple answer is the **newest your** router **supports**. If your router only allows using of WEP or WPA encryption consider replacing it as soon as possible. Both of those protocols have known vulnerabilities that allow bad actors to access your network in mere minutes by using publicly available tools. WPA2 is the most common at the moment, but if you plan to change your router in near future get a device that supports Wi-Fi 6 and WPA3.

So, why are the „dangerous" ones still around? Keep in mind that the device connecting to the router also needs to be able to use the encryption protocol. It is not uncommon for a business to use a specific device that may only operate on an older protocol. If that is the case, consider creating an extra network for that device to operate to avoid compromising all of your 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

5. Make a separate guest network

„Can I use your Wi-Fi?" is a question you will hear sooner or later while running a business. While it is an understandable (and a totally innocent) request 95% of the time, there is never enough caution when it comes to security, especially when most modern devices allow the creation of a guest network with a couple of button presses. Remember: while your guests may have the best intentions, their devices may already be compromised without their knowledge.

6. Actually, use a password to protect your network ☺

While all of the above tips are important, this is the most crucial one. All of those steps won't work if there is no password, to begin with ☺ (you can learn more about safe passwords from our Best Practices toolkit).

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!

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