MAKE YOUR HOME SECURER

INFORMATION SECURITY WEEK

We've all got smart devices in our homes these days. Perhaps you too have a SMART TV, a robot vacuum cleaner, or home domotics that open your curtains in the morning and turn on your lights in the evening with an app. Follow these easy tips to improve the security of your home environment. For example, did you know that you can install updates in many of your devices automatically? Read about this and much more in this handout.

MAKE YOUR ROUTER SECURE

Check the management portal of your router. With larger telecom providers, you can now do this with an app. If you can't manage for any reason, call your internet provider's helpdesk.

1. Check in the app or management portal whether you have a firewall feature. Set up the firewall so that your devices are no longer accessible online and online hackers are kept out.
2. Devices are often supplied with default passwords, such as admin/admin or user/1234. These are all easy to find on online forums, so change them to strong passwords immediately after installing a router. You can read more about strong passwords below.
3. Set your router to install updates automatically, so that known security loopholes are closed. If you can't update automatically, set an update reminder in your calendar every 3 months. If there are no updates in the app, check the manufacturer's website for information about updates.
4. Make sure your WiFi network is protected with WPA2 or WPA3 as well as a strong password. This encrypts your network and protects it from unauthorised access.

STRONG PASSWORDS

1. It's essential that you use strong passwords to protect your accounts from unauthorised access. A strong password consists of a combination of letters (both capitals and lower case), numbers and special characters. Avoid using obvious words or personal information, such as your name or date of birth.
2. Use a unique password for each account, so that if one password is cracked it doesn't leave all of your accounts exposed. However, it can be difficult to remember all these passwords, so use a password manager. There are plenty of free options available, such as Keepass and Bitwarden.
3. If you're not confident about using technology but would like to be able to rely on a company that protects your passwords, choose 1Password or LastPass as your password manager.

MULTI-FACTOR AUTHENTICATION

Double security is better security. Multi-factor authentication (MFA) helps improve the security of your accounts considerably. It adds an extra layer of protection by requiring you to confirm your identity after entering a password with a second piece of identification evidence, such as an SMS code, an authenticator app, a fingerprint or facial recognition. This makes it much harder even for hackers who know your password to access your accounts.

SMART DEVICES

Smart devices connect to other devices and networks to make your life easier. If you use smart devices, make sure they stay smart by following these tips:

1. Check for updates regularly or set your router to install updates automatically, so that known security loopholes are closed.
2. If you can't update automatically, set an update reminder in your calendar every 3 months.
3. If there are no updates in the app, check the manufacturer's website for information about updates.

Pro tip: Set up separate WiFi networks at home and connect all your smart devices to one of them. This will isolate your main devices, like phones and computers, from potentially vulnerable smart devices.

SAFE DEVICES

If you're thinking about buying a smart device, don't just look at what it can do and how much it costs. Smart devices often collect sensitive information; they might have a microphone to record sound or a camera to record images, for example, and it's not always clear what happens with this information. For this reason, bear the following in mind when selecting your new device:

1. Get independent information about the security of the device by searching consumer websites or consumer magazines for reliable tests, known safety risks and user experiences.
2. If you buy a device without EU approval, you'll be purchasing a product that might not meet European standards. This could put the security of the product and warranty in jeopardy.
3. If you buy a device associated with a service, such as a smart doorbell or a security camera, check where the data is stored. If it's stored in the EU, European privacy and security rules apply. If the data is stored outside the EU, look carefully at the requirements this storage meets.
4. Ask the online store about the security of the device you want to buy or how to set it up securely. If no information is available, ask if a secure alternative is available.

WORKING ON A HOME NETWORK

We're often asked whether working from home is safe; yes, it is. There are obviously risks involved, but these have been limited by the measures we've already taken. VIRO's confidential data is stored on servers inside the company, in data centres or in cloud services, which can only be accessed via a secure connection. Below, you can see the most important measures that protect VIRO information, even when working from home:

1. A secure home network – Make sure your WiFi network is protected with WPA2 or WPA3 and a strong password.
2. Create a secure connection – Use the VIRO VPN to encrypt the connection to VIRO data, which makes it more difficult for hackers to intercept your data.
3. Your VIRO laptop is protected with a firewall and antivirus software, wherever you are.