VUB Information Security and Privacy

How To – Work from home securely

Owner:
Chief Information Security Officer

Contact(s):
ciso@vub.be

Most recent update:
22 March 2020

I. Overview

A “How To …” document provides information, hints and tips about a specific Information Security and Privacy (ISP) topic. It does not contain a mandatory standard/guideline. It provides information about how a standard/guideline can be applied.

It is a ‘living document. The quality depends partly on the feedback from its readers/users. The cover page gives the contact e-mail address to which feedback can be sent.

A “How To” document does not follow a formal consultation or approval process.

II. Hints and tips on working from home securely

As a new VUB homeworker, you have been taken out of your comfort zone. You are suddenly confronted with the organisational and technical challenges involved in working from home. Even as an experienced VUB homeworker, you often ask yourself questions about how you can work from home securely. The VUB aims to support you as much as possible with this.

This document lists a number of points worth noting to ensure better information security when working from home. They will not only help you to secure your work, but also to secure yourself and your family with your private internet activities.

II.1. Recognising vishing and phishing

Cybercriminals have learnt that the easiest way to obtain essential data such as your username/password is to ask you for them. They mislead you so that you give them this information in good faith. They use phishing to obtain sensitive information. This is done both via e-mail (‘phishing)’ and by telephone (‘voice phishing’, or ‘vishing’).

For instance, you may receive a call from someone saying that they are a member of the Microsoft technical support team. They claim that your computer has been infected. You are then asked to install (malicious) software so that they can help you. Or you may also receive a warning by e-mail saying that a package could not be delivered. The e-mail asks you to click on a (malicious) link. This runs the malicious software or malware.

It may take many different forms, but there are a number of tactics that are frequently used:

- Creating a feeling of urgency. Fear, intimidation or a simulated crisis situation are often used as a lever to convince you.
- Inspiring trust by forging messages from a trusted organisation. Think for example of e-mails that appear to come from your banks.
- Exerting maximum pressure to incite you to ignore standard security procedures.

To build up experience here, you can consult “Learn to identify fake e-mails” from Safeonweb. Here you will find tips on how to recognise a phishing e-mail.

At the end of the day, you are your best defence against these attacks.

II.2. Securing your home network

Most home networks use a wireless connection or Wi-Fi. That is comparable to the VUBNext Wi-Fi network on the campus. The VUB protects its Wi-Fi networks against all sorts of attacks. However, it is also important that you protect your own Wi-Fi network at home sufficiently. If someone with malicious intentions simply connects to your network, this can cause a lot of damage because all devices that are connected to the network are, as a general rule, considered to be secure.

The central point of your Wi-Fi network is the router. This appliance communicates with your own device through Wi-Fi signals. Every router can be configured. The procedure for doing this differs from router to router. However, there are a couple of settings that apply for all Wi-Fi networks. Always choose a strong password and a secure communication method such as WPA2 for your Wi-Fi network.

Not sure how to carry out these steps? Ask your internet provider, visit the help pages or the FAQs and check the documentation that was supplied with your router or refers to the supplier's website.

II.3. Use a Virtual Private Network (VPN).

The VUB offers a secure connection to the internal VUB systems if you are not on the campus. For this, the VUB uses a VPN solution (Virtual Private Network). This software establishes a secure connection between your device and the VUB network. All communication is transmitted through an encrypted virtual tunnel, which prevents cybercriminals from being able to intercept readable communications and thus capture the information.

The VUB requires all communications sent from outside the VUB network to devices that are connected to the internal VUB network to go through the VUB-VPN. However, this does not mean that you need a VUB-VPN connection for all activities carried out at home. After all, the VUB offers several services that are directly available on the internet. For example, Office-365 (OneDrive, SharePoint, e-mail, etc.), the helpdesk portal via ServiceNow, TEO, PAM, Owncloud, Canvas, CaLi, Pure and Ultimo can be reached directly without VPN.

If you need access to a more secured VUB service, then you can use the Pulse Secure VPN software provided by the VUB. If you have not yet installed this software, consult the "VPN-toegang via Pulse Secure" installation manual which you will find on the VUB helpdesk portal.
Don't forget that you can only use this package if you are a registered VUB-VPN user. You can apply to register easily via the "New VPN account" item on the helpdesk portal.

II.4. Use strong passwords

A strong password is always the first-line protection for your system. Use a different password for each thing: one for your device, another for your Wi-Fi network, yet another for your Facebook account, for your Gmail account, etc.

You can gain access to all VUB systems with a single VUB username and password. The majority of the central VUB applications that you connect to via your browser use a single sign-on or SSO. This means that you only have to log in once to gain access to all your VUB systems. As soon as you close your browser, you end your connection and your single sign-on process expires. At the moment, RACS and EasyPay, Pure and CaLi are the only central VUB applications that are not yet connected to this SSO.

We stress once again that you should never share your VUB password with other people and you should use a different password for each different service (VUB, Gmail, Facebook, etc.). Think about using a password manager for all your personal passwords, but it is best not to store your VUB password here, either.

Be sure to read the "How To – Password Management" on the Information Security and Privacy website.

II.5. Install updates promptly

Cybercriminals are always on the lookout for vulnerabilities in the software that your device uses. That applies not only for the software on your laptop or desktop, but also for the software of your television, baby phone, security camera, router for home use, game console, etc. connected to the internet. In general, this applies for all technology that can be connected to the internet.

The suppliers of these systems issue regular updates to remedy shortcomings in their software. These not only install new functionalities on your system, but also resolve known vulnerabilities which endanger your information security. Consequently, it is extremely important to install all these updates, preferably using an automatic update function if one is available. Above all, take care that you only use official supplier sources for these updates!

Of course, the "update ready to be installed" notice always appears just when you're hard at work. You really don't want to restart your computer just then, so you click on the notice to remove it. It is important to realise that this makes it far easier for cybercriminals to hack your system. The success of cybercrime is fuelled by the race between cybercriminals and updates. So don't remove the message. Install the update as soon as it becomes available and make a virtue of necessity: take a short break while the update is installed.

Software that is no longer supported by the supplier no longer receives any security updates, either. Old operating systems such as Windows XP or Windows 7, old e-mail programs or any other software that is no longer supported constitutes a major security risk. You are therefore not permitted to used software that is not supported. Exceptions can be made for systems which cannot be replaced or for which a replacement is too expensive, but in such cases, adequate measures must be taken to limit the risk. If you are responsible for a system like this, always check what should be done with your Chief Information Security Officer, ciso@vub.be, and always do that before you carry on using the software that is no longer supported.

II.6. Use secure communication channels

Means of communication are important when working from home. As we said earlier, the VUB-VPN enables you to connect to the VUB network from home. But there are also a great many other means of communication. What is extremely important is that you make a very clear distinction between private and work communication and above all, that you don't mix the two. For your work communication, it is best only to use applications that have been selected by the VUB.

For individual or group discussions, you can use Skype for Business or preferably Microsoft Teams, which came into operation recently. You can start up both applications together with your operating system. You should select this in the settings of both applications. Then colleagues can contact you whenever they need to via these applications. Do not use any other applications for work discussions. Skype for Business and Teams both meet the VUB security requirements. However, for the alternative applications this is not certain.

If you send e-mails for your work, only use your VUB account. Sometimes it seems handy to quickly send a file to your own Gmail account so that you can print it locally, or e-mail your document directly to your local printer, if it supports this function. Remember that this means VUB information is spread over various locations. But these locations do not always meet the VUB security requirements and this can lead to leaks of sensitive information. So don't do it under any circumstances! Only use your local printer if it is connected to your system so that you can print directly.

If you surf to websites, make sure that your browser always uses an HTTPS rather than an HTTP connection. Definitely do this if you have to enter your personal data on this website, such as your username and password. HTTPS uses encrypted and secure communication. This is not the case for an HTTP connection, whereby all the data you enter are sent via the internet in full and without encryption and can consequently be intercepted by cybercriminals.

To help with the work you do at home, some colleagues may give you their (private) mobile number. Remember that you have only been given this number for work-related communication. Do not use this number for other purposes and certainly do not pass it on unless your colleague expressly agrees to do so.

When working from home, the boundary between using your (private) social media and work activities is not as obvious as it is at the office. Putting minor work details or your daily routine on line seems less odd when there are no colleagues with whom you can share these things. People working from home have to watch out for this, because updates like this often provide valuable information to set up phishing campaigns.

II.7. Be sure you have an up-to-date antivirus

Your system must have an active and up-to-date antivirus that automatically installs the virus updates. This is essential for the security of your system.

The VUB offers all its staff and students McAfee Endpoint Security. You will find the McAfee installation instructions here.

II.8. Protect your work system from children and guests, as well.

At the office, you don't have to worry about children, guests or other family members using your work laptop or your own systems on which you work for the VUB. When working from home, be sure to make it clear to your family and friends that they cannot (always) use your work systems. Such use poses a serious risk: VUB information may be accidentally deleted or modified or in the worst case, the system may be accidentally infected.

II.9. Finally: always use your common sense

Ultimately, every staff member is expected to use their common sense to be able to work from home securely. And if you have any questions, do not hesitate to ask. If in doubt, send an e-mail to helpdesk@vub.be with your questions: our helpdesk is always ready to assist you to work from home securely.