RSSI - Good practices guide

EDITORIAL

Smartphones and computers have become essential in our lives, but they have also become an important source for the dispersion of personal information.
To a large extent because digital technology has changed our daily behaviour. In our new virtual society, the need to exist through the eyes of the others will push us into intense activity. And rather than privileging real life one-on-one, many of us prefer one-on-one on our smartphone screen.

It is with him that we first share our photos, our emotions and our private life.
When you walk in a public space, all you have to do is lift your head and look around. You will discover all these people who slide their finger on their screen to scroll through content to see how others have reacted to their posts. This thumb up that will act on our mind as a reward that we were hoping for.

But, this dependence will also enable us to target both the contents, but also our quick reaction to allow intrusions into our personal and professional digital environments. Because of this permanent use, it is extremely important to ensure your digital security.

Olivier BOGAERT
Computer Crime Unit Commissioner - Federal Police

#1 BYOD

BYOD, with some precautions

BYOD is the abbreviation of 'Bring Your Own Device', which refers to the practice of using your personal equipment to access networks / services made available by universities. BYOD refers to usage scenarios in which the university's IT department has no control over the used device. Lack of control is precisely what IT people don't like.

Security for all
Let us give an example. When we go bowling, either we have shoes that are checked for conformity by the staff or we use the ones that are made available to us. We cannot use our dress shoes or our sneakers on the alley at the risk of damaging it.
If you are accessing an internal application or service from a device which is completely unknown to the university's IT department, it is legitimate to be concerned about its status and configuration. The goal is to ensure that its use does not put the users, their data, or their colleagues at risk - in short, to all the available IT services.

When we use a company computer, it is "managed" and applies a whole series of settings which together provide guarantees. Using a personal device means unknown factors. This does not imply that it is a problem but to be concerned is legitimate.
Beyond the aspects relating to its configuration, the personal device (the laptop or the USB key) is often shared with the whole family, which can lead to expose your personal, professional data and also those of the university to particular risks, mainly in terms of confidentiality. You have nothing to hide, fine, but the GDPR (General Data Protection Regulation) does not agree with that.

BYOD at the University

In business, the use of a personal device is relatively new, while at the university, access to IT services from completely unknown devices is not new. However, the multiplicity of devices as well as the permanent connection give another dimension to this question which deserves specific recommendations.

I have a University computer, is BYOD relevant to me?

The user is concerned as soon as he is in charge of setting up a device: computer, smartphone, tablet. Even though he has a University computer, this is not his only way to access the IT services: email on his smartphone, a management application from his home computer, etc. Therefore, the special provisions that are important to consider in a BYOD context apply to everyone.

What specific provisions are we talking about?

First of all, the used device must be well guarded in terms of configuration and protective measures. Then, certain practices must be avoided or adapted. Let us consider several aspects ...

The importance of updates

An operating system represents tens of millions of code lines, and a web browser is between 5 and 10 million. The complexity is such that it is impossible for these developments to be error free and some of them lead to security holes.

From this we can deduce two things:

1. Updates are the only way to correct program and system errors and security vulnerabilities;
2. when you add an application to your device, you add errors and therefore security vulnerabilities.

Update your device as soon as it offers you to do it and only install the applications that are strictly necessary. Avoid, for example, multiple programs that do the same thing (browser, email, etc.). Also, be sure to use the applications recommended by your IT department, they are the ones that will offer you the best solution in the specific context of your institution. Finally, and this mainly concerns your smartphones, reduce application access to what is strictly necessary (Do Messenger or WhatsApp really need to access your geolocation?). In this we apply a fundamental principle of information systems protection: that of "least privileges".

"But, I don't need the latest version of Word. All I do is type text! "

We are no longer talking about a security patch, but the overall evolution of versions software and operating systems. The IT world is changing very quickly and threats with him. An overly old application or system may become quite unsuitable. Even though it may not be justified from the point of view functional, even if it may seem abusive from an economic point of view, put update your systems and software to a recent version, this is necessary from the point of security view.

An antivirus on all devices?

Yes, and a firewall too! Generally speaking, the virus is a program that runs on your device for the benefit of someone other than you and always at your expense. The antivirus prevents, as much as possible, malware executions. Just like flaws and mistakes are present in all systems, viruses exist in all systems.

Even if you have a Mac, even if you are using Linux, use an antivirus. It does not solve all the problems, but it is a minimum.

The antivirus is a guard that watches over the execution of programs, the firewall is a guard that watches over the network. His role is also very necessary. Fortunately, your device usually comes with it as standard, just be sure not to turn it off.

Physical security

When it comes to protecting computer systems, we often hear: "If there is no physical security, there is no security at all." This expression is based on the fact that if an attacker has physical access to a device, it will not take long for them to gain access to all of its content. A little research on "forgotten password" followed by your system "Mac", "Linux", "Windows" should be able to convince you. Today, encryption systems can be used and partially overcome the risks associated with physical access to hardware. However, in keeping with the basic “in depth defense” principle, physical security should not be neglected.

Do not leave your laptop, phone, or tablet lying around, especially if they are not encrypted, but we will get to this later.

When we imagine the risk associated with physical access, we often imagine a hacker who dismantles the device, acts on the keyboard, connects it to a computer, plugs in a USB key or another device. You rarely see yourself intervening, and yet this risk is very real. Be aware that a USB flash drive or any device plugged into your device can be a vector for malicious content. A good idea here is to turn off the AutoPlay, this feature which automatically initiates an action when inserting a device.

On the home computer or on the phone which stays in my pocket, you do not need a code then!
Strictly, if you were certain of always controlling physical access to the device, you could do without other protective measures. However, let point out this basic principle: focus on the importance of the device contents and the reason why it is better to implement several measures to protect it.

Your home computer, your phone, your laptop, "Your Own Device" probably does not contain data that is not saved elsewhere on a cloud service or on University servers. This could lead to neglecting its importance because if you lose it, you lose nothing in terms of data. But, besides the issue of the content disclosure, which can lead to a more or less serious confidentiality problem, it is also the entry point to all your IT services. This device potentially holds the keys to all the doors, the passwords to all your services, and therefore has the value of a safe. This could be the saving of browser passwords or a password management tool. So even though it does not inherently represent a value or risk, we should deal with this personal device with due respect and use a code to protect its access. This code can take various forms, ranging from the traditional password, to biometrics, including the "PIN" identification code, dots to connect, etc. Be sure to use a code that is "strong". Don't overlook the complexity of your personal computer password and if shared, set up multiple users with disjointed workspaces. This precaution avoids the risk of your work data being intruded upon if, for example, your password is saved in the browser of a shared session.

When using your code, be careful that it cannot be seen indiscriminately over your shoulder.

If your device has a biometric solution, use it, it is the best solution combining protection and ease of use.
When it comes to biometrics, it can be useful to be able to deactivate it quickly, which is achieved by holding "power" and "vol +" or by 5 quick presses on "power" on an iPhone for example.
When is the access code requested? When the device is locked! Configure an automatic lock after a period of inactivity on your smartphone as well as on your computer.
Use a strong password or code on all devices, a biometric solution if possible, with automatic locking in all cases.

Encryption

As previously seen, only an encryption solution can compensate a physical security flaw such as the loss or theft of your device. In addition to the already mentioned questions relating to security, we must not neglect the questions relating to compliance, with the General Regulations on the Protection of Personal Data (GDPR) first and foremost.

If your device contains any personal data and it is lost or stolen, in the absence of an encryption solution, it is a data breach within the meaning of the GDPR, which must be subject to a declaration to the supervisory body. If you are using a recent iPhone or Android phone, its storage is encrypted, no worries, as long as it is locked with a strong enough code when lost.

If it is a computer, it is important to enable hard drive encryption. Each operating system offers built-in and simple tools to perform this function, but there are also quality portable and quality solutions between systems, including in the open source world. In any case, recent advances in both hardware and software enable the use of encryption to be (almost) transparent to the user.

Pay attention to the services you use

When it comes to compliance and beyond the device you use, there is the question of the services you consume. Do not forget that your responsibility may be involved in the processing of data, in particular personal data, which would be carried out by a service that you use and which would not be in accordance with the regulations in force. Familiarize yourself with the contractual terms of the services you use apart from what would be recommended (supported, validated and supervised) by your IT department, mainly in terms of confidentiality. The use of a solution outside any framework of your IT department is what professionals call "ShadowIT" and it is indeed not without risks.

BDNY or when "you Bring a Device which is Not Yours "

In the paragraph about physical security, it says in other words that "As soon as someone has physical access to your computer, it is no longer your computer”. What if, from the start, it is not your computer, like a public pc in a library or convention center? Is it safe to use it?

It all depends on what you want to do with it. If you need to search a bus schedule, no worries, but nevertheless use the browser "private" mode to prevent local recording of your activity.

If you are thinking at connecting to your email service, do not do it! You cannot have the slightest confidence in an unknown device, as far as the installed software or hardware are concerned. Spy programmes for instance, or even small devices that can be plugged in a USB port, are able to record everything you type on the keyboard, your password, for example.

Do not leave anything, in terms of data or files, and do not give anything, in terms of access codes, personal or confidential information when you are connected to a public computer!

I never connect to an unsecured network!

Whether or not a wireless network is secure has no direct impact on whoever uses it. Indeed, the secure side of the network is mainly about how to connect to it. An unsecured network is accessible to everyone; a secure network requires a code to connect to it. Beyond the connection, the risk associated with using a wireless network mainly depends on what you do with it because data security is not ensured by the network, but by the used application[1].

[1] A shortcut is taken here, because strictly speaking, the security of a wireless network relates to two aspects: the access and the encryption of the exchanges that take place there. The network therefore plays a role in data security, but this role remains local to the concerned wireless network. If we consider a typical use across the Internet, data security must be considered at the application level. In this case, it does not matter whether the wireless network used is secure or not, since the protection envelope is provided at another level and covers the end-to-end data exchange.

Virtually all communication on the Internet passes through a space over which both the sender and the recipient know nothing and have no control. The exchange is secure with applications which provide data exchange encryption, not at the "transport" level.

It is therefore better to use a secure application on an unsecured network than the contrary. To give a classical illustration, if you access an application from your institution with an https address validated in your browser, it does not matter whether you are on an unsecured network, the exchanges are encrypted and therefore unreadable for other users of this network.

However, a reservation on the open nature of the network must be expressed. Since anyone can connect to it, any behaviour is potentially possible, making it a potentially aggressive environment and against which your device should be protected. The protections mentioned earlier, including updates, a firewall and antivirus, are important here. In all circumstances, your device must be "well-kept".

Either way, always think twice before connecting to open networks you don't know: they are one of the most direct ways to collect information about you, or even compromise your machine. For one thing, there's a chance that a good deal of your network activity cannot be encrypted and even when it is, the fact that the network operator can analyze it gives him valuable information about you, even without being able to access to encrypted data. Finally, and without going into details, there are techniques which also make it possible to compromise the application encryption when controlling an obligatory passage point of network traffic (as it is the case for the operator of an access, Wi-Fi network or whatever). So, it is well worth thinking twice before considering to connect to an unfamiliar open network.

VPN: network access security

Let us start from the beginning. A VPN is a Virtual Private Network, which has its origin in the following situation: you work in a company that has its own network where internal servers are connected. The business is connected to the Internet, but all servers or services are not accessible from the outside for various reasons.

In order to enable access to an internal service from an external connection, a user can use a VPN connection. The VPN will establish a kind of pipe through which the connections will pass to the company network. From there, everything goes like if the remote computer was in the company, from a logical point of view. It can therefore access all local resources that are not “published” on the internet.

For our universities, this is often the case for bibliographic resources for example. Moreover, since the VPN enables to make believe a computer is elsewhere, it has other less glorious uses, such as bypassing restrictions on video-on-demand catalogs, ...

In summary

- Updates
- Minimum applications / supported applications
- Antivirus & firewall
- Physical security
- Access code & automatic locking
- Encryption of local data
- Services terms of confidentiality
- Be careful when using a shared network or computer
- Stay vigilant

In the near future, it is very likely that all of this will be simplified through Mobile Device Management (MDM). But in the meantime, it's your device and in a way, your responsibility. Implementing these recommendations can be simple for some and very technical for others. Do not hesitate to call your IT department to help you.

All of these measures apply two fundamental principles of information security: "in depth defense" and "lesser privileges" leading to a situation which provides very good guarantees. It is always possible to go further in terms of protective measures, but it will be at the cost of greater complexity of implementation and daily use.
And most importantly, after all that, there is what you make of it. There is no computer system on earth which, at one time or another, does not rely on a human being. It is at this level that the majority of attacks are carried out today. The device is now properly configured, let us not forget to configure the user.

#2 Authentication

Another important chapter is authentication. But first, let us define some important terms.

Definitions:

Authentication
Authentication is a process by which a computer system ascertains the identity of a user in order to authorize the user to access the system resources based on the rights assigned to them.

Identifiers
Authentication is done by means of identifiers. These identifiers are usually made up of an ID and a password. The ID is provided by the University and the users create a secret password of their choice.

Multi-Factor Authentication (MFA)
A Multi-Factor Authentication is an authentication that simultaneously implements verification processes using at least two different authentication factors. Some of the main authentication factors are: “what we know” (for example, a password), “what we have” (for example, a mobile device), “what the 'we are' (for example, the fingerprint). This can be described as a strong authentication method.

Authentication makes it possible to avoid experiencing particularly delicate situations
To understand the importance of authentication, let us take an example: "Alice is the research manager for her department at the University. She must therefore regularly access documents shared and stored on the University's online system. But Alice uses a simple password (Alice123) for her convenience. During a cyber-attack, hackers were able to guess this password quickly. They were able to encrypt all the work of Alice's department and now demand the payment of a ransom of € 100,000 to decipher these documents without which the whole department is paralyzed! "

What to do to avoid being in difficulty?
Here are the basic rules that must be observed:

- Choose a password consisting of a maximum of characters
- Mix letters, upper and lower case, numbers and special characters to compose this password
- Never communicate your identifiers to anyone
- Use different passwords for each application is ideal, but at least use a different password depending on the security levels required (Bank vs DIY site)
- Change your password regularly
- Use a multi-factor system if available

Good to know
A complex password can be easy to remember if it consists of a personal phrase. The "password" is dead, long live the "passphrase". Don't use a word, use a phrase. The sentence will be meaningful to you, unlike a complex word, and will be easy to remember. It will take a bit of a while to type at first, but the password you put together is so strong that you will not have to change it, so you will have plenty of time to get used to it.
And so that it is really very "strong", add your own personal "encryption key" in your sentence: for example, you replace the "i" by "1", the "e" by "3" (do not do this strictly, this is an example). The idea here is to keep the principle of the sentence by ensuring that its elements are no longer really words within the meaning of their existence in the dictionary.
The result is a great password that is easy to remember and will quickly become easy to type in use.

Multi-factor authentication is available in Belgium through the FAS (Federal Authentication Service), either through the electronic identity card, or through applications such as "ITSME". There are also AMF systems based on international certification systems such as "Memority", "Microsoft Authenticator" or "Google Authenticator".
In addition, password management applications such as Keypass or 1Password are also available. Be careful, these password managers will contain ALL your passwords and therefore if you lose them, you will have to change ALL of them!

#3 Social hacking

"It's not the technology that traps us but too often our emotions”

Many solutions exist in terms of IT security, but our behaviour remains the best shield against risks in terms of cybersecurity. We know that our brains are ruled by our emotions and rational thoughts, which makes us vulnerable to those who are evil intended and also makes us potential victims of
piracy.

Cybercriminals' modus operandi can inspire fear or curiosity, but the goal is to get you to achieve actions that you would probably not have executed in another environment. In effect, rather than hacking our computer equipment, it is easier to get our password by asking us.
Through harmless communication, we usually provide a lot sensitive information about us. This technique is social engineering. This can happen in the context of an insignificant conversation, during an exchange on social networks. Often security issues are deduced from this sensitive information we disclose (important date, favourite sport, etc.).

Protecting yourself well is worth it. With the right information, we can all do it. Internet security can seem complex to us and therefore we often ignore it. By adopting a way of thinking focused on
security, we will be able to manage it better. Caution lies between practice and security.

Social engineering is a technique that aims to access confidential information or computer equipment through directly or indirectly manipulating people.

Many of these scams start with e-mail. It is the most common way to send Internet correspondence.
It is easy to design a email that seems is coming from a known organization.
However, the veracity of the name and information associated with an address is never guarantee.

The electronic messaging system has no security system. This translates as follows:

- there is no way to verify the identity of the sender or the nature electronic mail;
- all elements of an email are falsifiable and easy to manipulate;
- emails sent are by default not secure and can be read or modified during delivery;
- e-mails can contain malware.

With e-mails, be calm and lucid, take your time and especially consider the following points:
Do you know the sender?

- Is the sender's domain name suspicious?
- Is this letter expected?
- Is the subject related to your activities?

It is essential to systematically ask yourself these questions. If in doubt, notify an IT consultant.

Other manipulation elements must also be taken into consideration: invoices or abnormal attachments, emergency call, strange or hidden web link, spelling mistakes, inheritance announcement, etc.

Even if the message seems genuine to you, caution and a little judgment reduce your risk of harm:

- think before you click and resist the pressure that hackers exercise to extract information from you;
- beware of emails. They are not trustworthy. Be critical;
- don't be afraid to contact an organization to check.

Social networks enable information to be exchanged. It’s also a factor of socialization, but they present new risks. The big names of social networking software (Facebook, LinkedIn, etc.) offer several settings to control the privacy of your profile and your interactions. Take time to learn about these possibilities. The options configuration may take time, but they are essential to increase your account safety. So only your friends or lists of specific people will be able to see your posts and private information. Take back control and never use default settings.

Another threat which combines the use of an email and your browsing is extortion by blackmail. Hackers may threaten you to surrender public confidential information about you if you do not take an action for them. It is important to remember that confidentiality and anonymity do not exist on the Internet. Regardless of the used technology or platform, the use of information technology always leaves its mark.

Usually, you will receive an email threatening to make public some confidential information about you if you do not pay. They also claim that they have successfully infected your computer and have been able to access compromising information (for example on the fact that you visit adult sites).

These blackmailers generally do not hold any compromising data on you at all They may have some information about you like a password you are using or have used. You need to know that this kind of information is unfortunately available on the Internet because of data leaks from certain websites that you use. No need to enter your computer to get this information.

What should I do?

- Do not panic
- Do not pay
- Change your passwords if you have any doubts

Remember a security-oriented way of thinking will be your best ally on the Internet: your common sense is your best defense system.

#4 Software and hardware

“My computer has been hacked! "

Alan has just received a visit from his IT support, who has detected an abnormal behaviour of his computer. After verification, it turns out that several malwares were installed without him knowing. It could have been worse: all his files could have been cashed against ransom, erased, even stolen and resold...

How is it possible?
As briefly explained in the previous chapter, if phishing (a technique used to obtain personal information in order to perpetrate an identity theft) and social engineering are the vast majority of successful cyber-attacks, cybercriminals can also exploit weaknesses in our computers, rather than manipulate the users themselves.

Our computers can be vulnerable. The software has become a monster of complexity, which inevitably leads to errors and flaws. They are analyzed and exploited remotely to order our computers to perform actions without our knowledge, mostly aimed at installing viruses and other malware. Once done, the hacker can either contact the victim to cash in on restoring the health of the computer, either use the computer discreetly to attack others for example.

How to protect yourself from these vulnerabilities?
As we have seen, solutions exist. To carry out regular updates (of operating systems, applications ...), use a modern antivirus (be careful not to install only one, otherwise they can neutralize), or other protection measures like a firewall, a antimalware or encryption of your hard disk (ask your local IT support team).

Despite all these precautions, my computer is infected ... what should I do?

1. A good initial reaction is to disconnect your computer from the network (wired and Wi-Fi). In this way, you cut off the hacker's access to your computer, viruses are not likely to spread to other computers on the network, and the infiltration of your data is not possible.
2. Also disconnect your USB storage devices (hard portable drive...), and check in parallel if the data of your backups has been affected.
3. Contact your IT support. Your professional data such as your private photos from the last 10 years are too valuable to leave things to chance.

#5 Securing data

We all handle large amounts of data in our daily work. Whether it is just our emails, research results, publications or reports, they often need to be protected in a way adapted to their nature and to the constraints that are attached to them.

The choice of a medium

The choice of the computer data medium will obviously depend on their nature and how they will be used. Most of the time, the storage on an institution computer is sufficient for your emails or personal documents, but the question becomes trickier when considering sharing data with collaborators.

In all cases, however, if you are sharing a medium containing sensitive data (in the sense of privacy or intellectual property for example), it will be necessary to encrypt the data by cryptographic means (see below).

Removable and / or portable media

Depending on the size, the use of an external hard drive, a simple USB key or a memory card (eg SD) may be useful but requires special care: by its nature, such a medium can easily be stolen, lost or damaged. This is also more generally the case with laptops which are often used as the first means of storage. It will therefore be necessary to ensure the backup (we will come back to this) and the physical protection: personal surveillance, closed doors, security locks.

Remote media

Using remote media not only enables us to access to our data from several workstations, but also to share them with our collaborators.

Favouring the use of institutional services must be considered as a golden rule! Whether it is Windows shares or private cloud tools (such as Owncloud / Nextcloud) or public cloud professional tools (such as Office365), the institutional infrastructure is secured by professional IT specialists and placed under the responsibility of the institution, in particular with regard to compliance with the existing legislation (i.e. GDPR).

If the possibilities proposed by the institution do not match your needs: discuss it with the IT department! The possible means and adaptations are not always known.
If you really are forced to use an external storage service: be careful! Free services (Google Drive, Dropbox, iCloud and others) must be avoided: "when it's free, you are the product". Please always ensure that you have a valid contract with your service provider and make sure you have data security clauses when defining the public market. The implementation of GDPR has added very important constraints in relation to the use of these services, the use of encryption (see below) should be systematic, by simple precautionary measure. Do not hesitate to contact the person in charge of computer security to be advised on this matter.

Data protection

Whatever the chosen medium, it is always essential, for shared data, to identify who can access it (read / write), for what use and for how long.

Access rights management
File sharing or collaborative editing services generally offer the possibility to fine-tune these access rights (do not use those who do not enable it). The specific definition of these rights (everyone can do what is necessary for him but not more: lesser privilege) and the management over time (for example when a employee leaves the project) represent very important issues for the management of your data and should be the subject of a specific responsibility within any project.

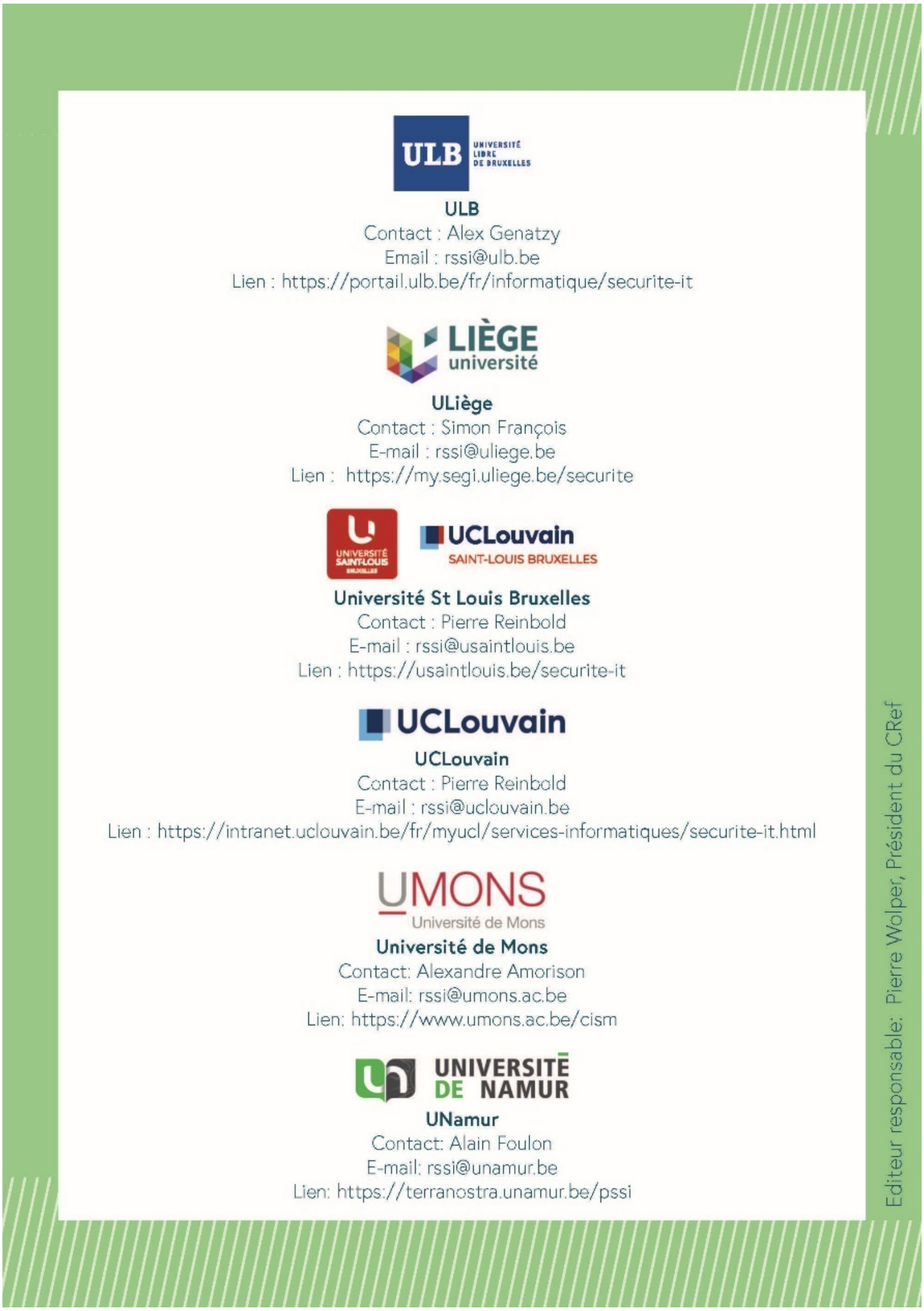
Cryptography and Encryption
When handling sensitive data, for example within the meaning of the GDPR for personal data, or valuable data, patents or more generally of intellectual property within the institution, the use of encryption should be considered systematically. Data encryption prevents any third party to read and use them. When handling sensitive personal data, the GDPR requires the use of encryption under threat of high penalties in case of leaks. The IT department of your institution offer solutions to implement encryption of your data in a secure manner.

Typically, these cryptographic solutions generate some additional constraints, such as the management of encryption keys, which must be secure, or a stronger authentication, for example, using a text message confirmation in addition to a login and password. Depending on the chosen solutions, these constraints will be more or less strong but require your personal involvement to be effective. It is necessary to remember that in the event of loss of the encryption keys, it is simply no longer possible to access encrypted data!

The use of cryptography in your institution addresses this problem globally to ensure that recovery of encrypted data is still possible.
In terms of cryptography, as with all computer security, "security by obscurity does not exist". Always favour software that uses well-known and proven algorithms. Open-Source solutions, with a code that can be audited, should be used preferentially.

Data backups
Whatever the level of security of your media or tools, data backup requires special attention. You must have regular, automatic and securely stored backups. As always, favour the use of institutional services. Although it is often very easy to buy and install an inexpensive external hard drive to perform backups, it constitutes a potentially very sensitive data medium and must be secured as such (see above). The backup of your professional data should be placed under the management and responsibility of the institutional IT staff.

Data lifecycle
The data that we handle in the course of our work is often associated with specific conservation constraints: the duration of a project, the time of a thesis or sometimes longer for archiving. Your data lifecycle should be defined from the start: from acquisition to archiving through storage. This is an opportunity to define the appropriate security measures for each of these steps.
Archiving or destroying data at the end of the project is an important step which should not be overlooked.



ULB
Contact : Alex Genatzy
Email : rssi@ulb.be
Lien : https://portail.ulb.be/fr/informatique/securite-it

ULiège
Contact : Simon François
E-mail : rssi@uliege.be
Lien : https://my.segi.uliege.be/securite

Université St Louis Bruxelles
Contact : Pierre Reinbold
E-mail : rssi@usaintlouis.be
Lien : https://usaintlouis.be/securite-it

UCLouvain
Contact : Pierre Reinbold
E-mail : rssi@uclouvain.be
Lien : https://intranet.uclouvain.be/fr/myucl/services-informatiques/securite-it.html

Université de Mons
Contact: Alexandre Amorison
E-mail: rssi@umons.ac.be
Lien: https://www.umons.ac.be/cism

UNamur
Contact: Alain Foulon
E-mail: rssi@unamur.be
Lien: https://terranostra.unamur.be/pssi

Editeur responsable: Pierre Wolper, Président du CRef

UNamur contact: Alain Foulon - rssi@unamur.be