Bureau
Telecommunicatie en Post

Cyber-Security Awareness Program

October 2018


CYBER
SECURITY
CONFIRM
click here for more information

Contents

Introduction

Many companies and organizations depend more and more on the Internet and computers to be able to produce their products and/or offer their services.

The use of the Internet and computers makes work more efficient. However, as companies become more and more connected, they should also become more aware of the cyber-security risks for their organizations, including all kinds of vulnerabilities of the software and hardware their company is using. These vulnerabilities, when manifested in security incidents, can lead to data loss, information leakage, online fraud and so on.

Consequently, a company can lose valuable company data or suffer financial loss and reputation damage. No matter what the level of incident or breach might be, it can be devastating for the company and its employees.

Cyber-security guarantees:

- Confidentiality of information
- Integrity of information
- Availability of systems

Every company should have a cyber security policy and a cyber security plan in place. Cyber Security consists of different intertwined measures, like physical security, network security, computer security, and more.

The effectiveness of these measures will be determined by the way the company's employees will comply with the measures implemented by the company. Every employee doing work under a company's control must be aware of the cyber threats and cyber risks, but for that, first they need to be informed and made aware of these threats and risks, as well as of the company's cyber-security policies. Cyber-security policies and awareness programs should always be communicated in writing.

In this booklet, the BT&P offers a simple cyber-security awareness program outlining what employees should do and, of course, what they should not do. This security awareness booklet is meant as a simple and easy-to-use guide for the whole company.

Chapter 1. Protection of company data and assets

1.1 Information classification

As technology progresses, it brings about an evolution in the way we work. With the introduction of mobile technology and BYOD (Bring your Own Devices), comes an expansion of the threat landscape. This means that cyber attackers now have a larger, more varied platform to use for their attacks, because an environment that used to consist of mostly Windows machines and a few Linux servers can now also include Android and iOS devices in a variety of versions. Protecting your environment in its entirety is a challenge.

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Examples of confidential or sensitive information are human resource management information, financial management information, legal documents, and so on. Companies should identify confidential and/or sensitive information in their company and define the right policies to handle this information, which most of the time is valuable to the company. All confidential/sensitive information should be labeled accordingly, and employees should be aware of the fact that unauthorized disclosure of confidential/sensitive information might cause harm to the company.

Not all business information is created equal. Information has varying degrees of confidentiality and sensitivity. Employees should be educated about the level of sensitivity or confidentiality of the information your company works with. The confidentiality and sensitivity of a document can determine with whom you can share and/or discuss the data it contains.

We should be careful which information to send via e-mail and to whom it is sent. E-mails are often sent in clear text (human readable), which can be intercepted and leaked. Confidential or sensitive information should not be sent in clear text via e-mail. Print and copy documents only when necessary and, while doing so do not leave the printer or copier unattended when printing or copying your document. Make sure all hardcopies are filed and stored in a safe place or shredded after they are no longer needed.

BE AWARE OF THE FOLLOWING!

- Confidential/sensitive data should be labeled properly.
- Labeling should always be clearly visible on each confidential/sensitive document, either digitally or by a stamp.
- Never read, take, copy or print confidential/sensitive information without authorization and/or share and discuss it with other unauthorized persons.
- While printing/copying confidential/sensitive information, never leave the printer or copier with the information unsupervised.
- When copying confidential/sensitive information, always check the copier not to leave any information behind.
- All printed confidential/sensitive information should be kept under lock and key.
- Confidential/sensitive information must always be disposed of by shredding.
- The company should hold a record of all dissemination of classified/sensitive information.
- Never send confidential/sensitive information out of the company without company's approval and certainly never via email.
- Never share confidential/sensitive information without authorization via telephone or email with unauthorized people, and certainly not in public areas, with the press if unauthorized and, finally, never share such information with family and friends.

1.2 Passwords

One of the oldest ways to protect computers and digital devices is by using passwords. However, because passwords have been around for a long time, there are plenty of ways to circumvent them, especially "weak passwords." When it comes to passwords, everyone has a difficult time remembering them, yet they are an essential and sometimes the only factor blocking access to networks and information. Passwords are the guardians of our information – but who is guarding the guardian? A security measure (in this case a password) can only be effective when it is used and guarded properly.

One of the most common password-related errors is using "weak" passwords. Most of us are tempted to create simple and easy to remember passwords. However, simple and easy passwords have a high risk of being compromised. One of the most common password attacks is password guessing. In this attack, the attacker will try to guess the victim's password. The simpler the password, the easier it is for an attacker to guess it. Another attack example is shoulder surfing: this is when an attacker tries to see the password being typed by the user, standing behind/beside the user. An easy password can be obtained with minimal effort using this method.

Passwords must be kept secret. Next, some of the challenges to creating passwords will be discussed and some possible solutions to these challenges.

Creating new, strong, but easy to remember passwords is not simple. A strong password is a password with a combination of uppercase and lowercase letters, numbers and symbols. Furthermore, best practices show that passwords should be long enough—18 to 21 characters is the standard (in most cases). However, an employee should stick to company policy if different. When passwords need to be long (18-21 characters) it is best to use a sentence. The password is then called a passphrase.

One option is to take a favorite song, poem or quote and add some changes to the sentence with "replacement rules." If you want a strong password that is both short and easy to remember you can use "replacement rules."


Sign in
Username
user
Password
Sign in

For example the quote “Be the change you want to see in the world” can be modified with the following rules:

1. Take all the first letters of the words in the quote and capitalize them: **BTCYWTSITW**
2. Change some of the letters to numbers: 8TCYWT51TW
3. Make some of the letters lowercase (you can make every other letter lowercase): 8TcYwT51tW
4. Add some symbols:!@8TcYwT51tW#$

   For a longer password or passphrase, the following replacement rules can be used:

   1. Change letters into numbers:
      B3 TH3 CHAN93 Y0U WANT T0 S33 1N TH3 W0RLD
   2. Change some letters to symbols:
      B3 TH3 CH@N93 Y0U W@NT T0 S33 1N TH3 W0RLD
   3. You can make it shorter by replacing whole words with single letters or numbers that are phonetically the same. In our example the word “T0” can become the number 2 and S33 can become the letter C. You can also remove the spaces between the words:
      B3TH3CH@N93Y0UW@NT2C1NTH3W0RLD

It all depends on what you want the password to be. These techniques take some practice. However, once you learn to remember your “replacement” rules, it will be easier to create and remember strong passwords.

In this day and age even the average computer user has many different passwords and it is close to impossible to remember them all. Writing them down often becomes the most used option, however if you do write them down, make sure you put them in a place that only you can access, for example a file cabinet with a sturdy lock and you being the only one in possession of the key. Do not place your password in plain view, and definitely do not “hide” it under your keyboard, mouse, laptop, screen or any other place where someone can search and easily find it. Just remember, a determined person will look everywhere in order to find your password. Furthermore, if you do write down your passwords, don’t go around telling everyone about them and where you stored them. Also make sure to always put them away as soon as you are done with them.

Password sharing is very dangerous and unnecessary in a properly managed network environment. If an employee needs access to some information, the administrator (employee of IT Department) should be able to provide it without requiring another employee to reveal his/her password. In the event that an administrator can't do this, proper documentation should be created and signed to protect the employee who has to share his/her password. Once the situation that required the employee to share his/her password has been fixed, the employee's password must be changed immediately.

BE AWARE OF THE FOLLOWING

- At all times, all employees should be able to create their own passwords to access information on the company's network or to access confidential/sensitive information.
- If an employee suspects or knows that somebody else knows his/her password, he/she should immediately change the password or request a new one.
- Passwords should not be written on post-its or stuck around the desk. If an employee can't avoid writing them down, they should be locked up in cabinets with proper locks.
- Employees should never reuse their office usernames and passwords for their private accounts.
- Employees should never share their passwords with their colleagues or their managers. If managers need access to the in formation, the IT department can provide management with proper access to the information easily. In the event that someone does use an employee's passwords to access information, these should be changed immediately after.
- Never share passwords via email messages or telephone.
- Never save passwords in mobile phones or tablets.
- Never use the option "remember this password" in programs or web browsers.

1.3 The desktop computer

Nowadays, a (desktop) computer is the most important office tool. For everything we do, we need a computer. If a computer is defective, we must call the employees of the IT department, and they take care of it. So the IT department is the one responsible for making it work again. Even so, cyber security is everybody's responsibility, since we are all vulnerable to cyber-security threats.

BE AWARE OF THE FOLLOWING

- When an employee is not at his/her desk, he/she must always lock the computer. This can be done easily with  +L.
- Laptops and portable computers can be secured physically with a laptop locker cable or put away in a cabinet with a lock.
- Always shut down computers completely when going home at the end of the day.
- Never install new software on a company computer without permission.
- Report all unusual events on the computer to the IT department.
- When travelling with a business laptop, make sure it is locked with the proper password and encrypted if possible.
- Never give anybody access to your computer, unless you have explicit permission from management or the IT department.
- Never use a company computer for personal matters.
- Never leave laptops unattended in cars or at airports to prevent them from being stolen.

1.4 Mobile Devices

Nowadays, mobile devices are preferred more and more over desktop computers in the office, since they are portable. The objective of mobile devices is to be able to easily take them with us to meetings, to work at home, and when traveling. Mobile devices are laptops, tablets and smart phones. However, when you are on the go, it is easy to leave something behind, especially when traveling.

There are also thieves to take into consideration, as they never miss a chance to take advantage of a vulnerable device. Always pay close attention to your surroundings, don't leave your luggage alone when traveling and always make sure that you packed your devices before you leave a location. Even though we all know that we should lock our mobile devices at all times, we still tend to forget.

BE AWARE OF THE FOLLOWING

- Use a PIN/Password to protect mobile devices which contain company data like emails and/or documents. Refer to the user guide of the mobile device for instructions on using a PIN/Password for security.
- Be sure to remove all company data and information from the device if you stop using it.
- Always report loss of a company mobile device immediately.
- Never leave a company mobile device in the car.
- Never lend your company mobile devices to others, especially if they will be unsupervised.


esc
caps lock
ctrl
fn
alt

1.5 External devices

External devices are everything that is mobile and that can be connected to the (mobile) computer. External devices are CD/DVDs, External hard drives, USB sticks, and so on. Today, the most commonly used external storage device is the thumb drive (USB stick), but external hard drives are also very popular. Another very popular yet often overlooked external storage device is the mobile phone.

Although data storage is not its primary purpose, mobile phones can also be used to store and transport data. Furthermore anything that can store and transport data can store and transport malware (USB sticks, External Hard drives, Mobile Phones, CD's). Hence, great care must be taken when connecting these external storage devices to company computers. Make sure you know your organization's policy about using these types of devices and if they are allowed, always scan them for viruses prior to use.

BE AWARE OF THE FOLLOWING

- External media containing company information should be locked away safely.
- External media should automatically be scanned for viruses prior to being used on a company computer.
- The IT department should always scan an external device if it has been used on another network that is not the company network.
- Always report loss of external devices to IT department, with a list of the lost information.
- If you stop using an external device, always deliver it to the IT department so they can wipe or destroy it.
- Never share external media with others.
- Never insert external media from unknown sources into a company computer.

1.6 Clean desk

Sometimes we tend to think of cyber security as a complicated matter, and most of the time it is. Behind every computer in the office there is a network and behind every network there is a team of IT specialists working hard to keep the systems safe and running. But there are also simple steps users can take to ensure their data is secure. Not all cyber security measures have to be technical measures. Procedural measures are as important as the technical. Next, some procedural measures will be discussed.

One of the simple steps users can take is locking their computer when they leave their desk unsupervised. It is easy to think that only outsiders might want to get the information on your computer. However, there are also malicious insiders. These are people who work for the company who may not have access to the information you have. Leaving your computer unlocked while you take a break creates an opportunity for a possible malicious insider to get the data from your computer. There are different ways to lock your computer. However, on Windows systems there is a handy shortcut that makes locking your computer as simple as pressing two keys on your keyboard. These two keys are 1. the Windows button and 2. the L-key. Or you can go to START and choose Lock/Sleep.

Whether you are working on the go (mobile) or in the office, be mindful of what is going on around/behind you. Malicious or curious insiders can easily look over your shoulders to see information. A clean desk can prevent shoulder surfers and fast readers from reading information from an employee's desk.

Always make sure you store away all printed documents when you are leaving your desk. Most organizations have a “Clean Desk policy.” This policy dictates that all information pertaining to the business (printed documents, USB, hard drives, CDROM, notebook, post-it notes, to name a few) must be stored away once the employee leaves his/her desk. Be sure to lock your desk, file cabinet(s) and office when leaving the office and the desk is clean.

BE AWARE OF THE FOLLOWING

- Employees should lock up all documents and all confidential information when leaving the room, during all breaks, or when going home after work. The clean desk policy should be always enforced.
- All documents, external media and post-its containing any confidential information should be locked up in cabinets with keys.
- All cabinets containing confidential information should be locked up when the employee leaves the office room.
- Never leave confidential information written on “whiteboards.”
- If the maintenance department needs to be in the employee’s office, clean desk is mandatory.
- Clean desk is mandatory when there are unauthorized employees in the room, consultants and/or other visitors.
- Employees should not allow visitors into their offices. If by chance a visitor still enters the room, clean desk is mandatory.
- Keys and tokens that give access to cabinets or computers with confidential/sensitive information should never be left on a desk unattended.

1.7 Physical security and safety

All employees are responsible for the security of company data and assets. Each and every person has to take care of his/her own security, as well as help other colleagues to protect their data and assets. Physical security is as important as computer security, and it entails physical measures like guards, locks, signs and badges. The implementation of these tangible controls is also important.

BE AWARE OF THE FOLLOWING

- Employees should close all doors that need to be closed, therefore doors should have proper locks (smart card, cipher lock, biometric, or traditional).
- Visitors should receive an in/out badge and not be allowed to walk around without surveillance or an escort.
- All employees should know company policy related to visitors and explain such to their visitors so they can comply.
- When leaving the office, all cabinets, drawers, doors and windows should be properly closed.
- Additional intruder detection measures can also be used, like CCTV, motion detectors, metal detectors, and so on.

1.8 Public Wi-Fi

Wi-Fi has become readily available in coffee shops, hotels, and airports; even public transportation now provides free Wi-Fi for their always-connected clientele. However, because it is readily available and open for everyone, it is risky to use for business purposes, because with the proper programs, a malicious actor can see all traffic that passes on a Wi-Fi signal. Publicly available Wi-Fi without a password is unsecured. They are mostly free of charge, but pose a high risk to business users. If a Wi-Fi network is not password-protected, then it should not be used for anything business-related.

BE AWARE OF THE FOLLOWING

- Company laptops and other mobile devices should not be connected to public Wi-Fi networks without a password
- Confidential/sensitive information should never be shared via public Wi-Fi connections
- If for any reason, a company username and password has been used over a public Wi-Fi, like while traveling, they should be changed immediately after returning to the office.
- Never make confidential transactions via Wi-Fi.

Chapter 2. Protection against malware

2. Malware

One of the most popular methods for delivering malware (malicious software) is through e-mail. This can be done in two ways: 1. Malicious attachments or 2. Malicious hyperlinks.

One of the most common methods of infecting computers is through malicious attachments. Attachments are files that are attached to e-mail messages. There are various file types and all can be used as attachments. Some examples of file types are: .exe, .com, .bat, .docx, .docm, .zip. However, there are certain file types that tend to be favored by cyber criminals when they want to send malware. File types that are usually misused to send malware are .exe and .zip, because they are executables. These file types should never be opened when received without confirmation of the sender. It is better to contact the IT department to see if all security measures, like a virus scanner, are in place before opening an .exe or .zip file.

Another way that criminals try to hide malicious files is by giving a document two file types, for example invoice.pdf.exe. What makes this even more dangerous is that some computers automatically hide a known file extension, which means that the file invoice.pdf.exe is displayed only as invoice.pdf.

When clicking on these files and thinking they are a PDF, a possibly malicious executable (a piece of software) will run instead of opening a PDF file. It is important to note that files with double extensions are almost always malicious. If you encounter such a file, contact your IT department immediately.

Another common method for infecting computers is through hyperlinks. A hyperlink is a sequence of alphanumeric characters that can take you to a specific website. www.example.com is a hyperlink. Hyperlinks can be "disguised" or "hidden." This is primarily what makes hyperlinks so dangerous.

For example, you can receive an e-mail that contains a hyperlink: www.safesite.com; however, the actual path may be www.fakesite.com/download/maliciousfile.exe. To find out the true path behind a hyperlink, hover with your mouse over the link. Be very careful not to click on the link.

The goal of sending a malicious hyperlink is to get users to browse to a malicious website with a vulnerable browser. The website itself or advertisements (ads) appearing on the website can contain malicious software that uses the vulnerable browser to infect the user's computer.

Pop-ups are small windows that open when you visit a website. There are malicious pop-ups that try to convince you to click on them. To do this they may use scare tactics ("your computer is INFECTED! Click here to clean it for free!") or false promises ("you just won 1,000,000 dollars!") to get you to click on them.

Pop-ups are rarely a problem anymore because modern browsers include pop-up blockers that prevent the small window from opening.

However, it is very important that if you ever do encounter a pop-up to not click on anything. Not even the close button, as this could lead to an infection. The best course of action is to close your web browser and contact the IT department to install or reconfigure your pop-up blocker.

BE AWARE OF THE FOLLOWING

- Use the combination of the CTRL+F4 keys to remove the pop-up window.
- Pop-up blockers are installed automatically with browsers; if not, the employee should contact the IT department.
- Employees should not deactivate the pop-up blocker.

2.1 SPAM and digital chain letters

Cybercriminals have become increasingly skilled in developing malicious e-mail messages to trick the user into sending them his/her personal information. These fake emails come close to looking like real email messages, especially when it is a targeted attack (an attack designed specifically to target a company). It is important to be able to determine whether an e-mail is legitimate or not.

There are some characteristics that can help the user determine whether an e-mail is malicious and/or suspicious:

- The email is unsolicited, meaning the employee did not ask for it, was not expecting it, and doesn't need it for his/her work.
- The sender is unknown, or the employee has never corresponded with the sender before.
- The email instills a sense of urgency in the receiver, urging the receiver to act immediately or else something very bad will happen (for example an account will be closed, or you will be fined, fired etc.) The more urgent it sounds and the more dire the consequences, the greater the chance that the recipient will panic and complete the requested action.
- The e-mail contains suspicious "hyperlinks" that lead to different domains.
- If the e-mail contains a suspicious attachment with a suspicious file extension as mentioned in the segment "Attachments," then it is possibly a phishing e-mail.
- If the e-mail contains a generic title such as "invoice" or "report," it is possibly a phishing e-mail.
- Cyber criminals often hack legitimate e-mail addresses to use in their phishing campaigns. However, they often cannot hack e-mail addresses of the business they are pretending to be and will use hacked public e-mail accounts (for example a Gmail or Yahoo account) instead to send a fake "business e-mail." Also, if you receive an e-mail claiming to be from someone working for example at FEDEX, but the e-mail address used is a public e-mail address (example finance@juicyjuice.com), the email can be considered a phishing mail.


Email
Spam Email
Do not show this message again
Yes
No

- Another trick criminals use is to create domains similar to popular company names, using characters that look similar to try and trick the recipient. For example, they will make finance@legitimate.com into finance@|egitimate.com or finance@1egitimate.com. In the first fake address a “vertical bar” or “pipe” symbol is used instead of the letter “l” (side by side comparison with the letter “l” and the pipe symbol → letter, symbol: l, |). In the second fake address the number “1” was used instead of the letter “l.” So, the user should be very alert and check whether the spelling of the email address is correct. If the sender’s e-mail address has been disguised in this fashion, the e-mail is a phishing mail.

- Grammar in the emails can also be a sign of a phishing email. Although the amount of spelling errors can be minimized with spellchecking software, there are still sentence and other structural differences between languages. Sometimes criminals will try to translate the text from their native language to English using translation software. Translation software does not correct poor sentence structure. Due to this, the sentences in phishing e-mails may have bad grammar.

- If an e-mail contains a suspicious greeting line, such as using your e-mail address in the greeting, it is definitely a phishing email. For example, if your e-mail address is willem.stad@korsou.cw, the greeting would look similar to this: “Dear willem.stad” / “Hello willem.stad”/ “Hey willem.stad”.
- Correct business e-mails will contain a signature and or contact information other than the e-mail address, such as a phone number or a physical address. Phishing e-mails often do not contain contact information.

As discussed above, there are many ways to detect if an email message is malicious. However, as cybercriminals hone their skills, it gets increasingly difficult to recognize certain phishing e-mails. When in doubt of the legitimacy of an e-mail, just call to confirm.

BE AWARE OF THE FOLLOWING

- Always remove malicious email immediately. This can be done via a “remove unwanted emails or spam” option included in many email systems or via the firewall administrator.
- Never forward malicious email messages to others.
- Never click on links you find in malicious emails.
- Never open attachments of the malicious emails.
- Never use the company email account to do personal online shopping or use these credentials to register with other websites for personal use.
- If you receive an e-mail and you are unsure of its legitimacy, it may be possible to contact the organization and ask for the person that sent you the e-mail. Make sure to use a publicly available phone number, never the phone number in the e-mail (if one is provided).
- If the email was from an associate and still looks suspicious, the best thing is to call and confirm if the associate indeed sent it.

2.2 Phishing & Spear Phishing

We must be aware of Social engineering. Social engineering is the method of using different forms of social interactions to make people reveal sensitive information or perform an action they normally would not. Social Engineers take advantage of the natural human instinct to be helpful and to trust. One of the most popular forms of social engineering is Phishing, which is a technique used by cyber criminals in which they send (fake) e-mails with malicious attachments or hyperlinks.

They ask for personal information by posing as a high-level employee of the company (such as the CEO, CFO, etc.) or by posing as a well-known associate of the company. If the user clicks on a hyperlink, he/she might be redirected to a website where he/she is asked to login with a username and password. If the attacker targets a specific company by sending emails to one or more employees so that many of them receive the same suspicious email, this is called spear phishing.

BE AWARE OF THE FOLLOWING

- Phishing emails always have some kind of wrong spelling. Always check spelling and sentences. If they are not in correct English grammar, it might be a phishing email.
- Always be sure you know the sender of the email. Otherwise don't answer the email and don't open any attachments.
- Always be sure the subject is related to work before opening an email.
- If there is any doubt about the legitimacy of the email, always delete it. Do not be curious!
- If an email is supposedly from a company and the address does not match the email addresses of that company, then give the company a call to verify.
- Always check the email address by hovering the mouse pointer over the email address to see if it matches the name of the sender.
- If for any reason the employee has to follow a hyperlink, check the link before by hovering over the link with the mouse. The real address of the link will be shown. A small popup-window with the real address of the link will appear within that small window.
- Always inform the IT department if you accidentally clicked on a hyperlink or attachment in a phishing email.
- Never forward emails containing contents unrelated to work to other colleagues, like jokes, commercials, etc.
- Never send user credentials (username and/or password) via email or share by phone. These credentials are to be exchanged only person-to-person or encrypted.
- Even if an email addresses an employee by the correct name, that is no guarantee it's legitimate – you must still check to determine it's not a phishing scam. The employee should then check for incorrect spelling or grammar, or an unknown sender, in which case it's most probably a spear-phishing email.

Chapter 3. Segregation of duties

3.1 Network administrators

To be able to guarantee the confidentiality, integrity and availability of data and information systems, it is important to identify conflicting duties and areas of responsibility and make sure that they are segregated. Segregation of duties reduces opportunities for unauthorized or unintentional modification or misuse of the company's data, information and information systems.

Best practices show that it is important to separate the network administrators' role from that of regular users. Network administrators are users with the highest level of access rights to the network and computer systems. A user who is a network administrator has the rights to make changes to network, computer and security settings that will affect (all) other users. Network administrators can change security settings, install hardware and software on the computers, access all files on the computers, and make changes to accounts of other users.

The segregation of duties between network administrator and regular user can be enforced through access control. Access control is the process that gives permission to access data, information and files on the network through the creation of different user accounts with different levels of access. Network administrator accounts should only be granted to those with an administrator function/role in the company.

BE AWARE OF THE FOLLOWING

- The network administrator should never give other users the username and password of the administrator account.
- The network administrator should never leave computers unattended with the administrator account logged on.

3.2 Regular users

Regular users are all other users with no network administrator account. Users with regular user accounts do not have the rights to change security settings on computers, nor to install hardware and software on the computers. Regular users can only access the files they need in order to do their work and should not have access to other information on the network. Regular users, depending on their function, can access one or more compartments of the network. Access to information should always be minimized to guarantee unintentional changes to others' data.

BE AWARE OF THE FOLLOWING

- Never access information that you do not have permission to.
- Never give users without permission access to information on the computer.
- Never install private hardware and software on the company's network or on the company's computers.
- Never use an administrator password to grant unauthorized access to files you do not have permission to access.
- If additional access is needed to other information, this should be requested via the IT department.

3.3 All users should report irregularities

Never be afraid to report suspicious activities to the people responsible for data, information, IT systems and/or the network. Suspicious activity does not only involve activities on the employee's computer. Sometimes co-workers may also perform activities that are not allowed to, either unintentionally or intentionally. If you see something, speak up!

Chapter 4. Privacy and GDPR

Privacy becomes important when personal identifiable information is being collected, processed, used, stored, and/or shared. Privacy is the opposite of publicly, and can be online or offline. Online privacy is about the information that is collected digitally to be processed in ICT systems. The offline privacy is what the person is doing, saying or how the person is behaving in private. And also personal information on hardcopy is described as offline. The extent to which privacy of citizens is being valued depends on each country's culture. Each person has the right to his/her privacy.

Advancements in ICT affect our privacy in different ways. Some systems might collect too much information of a person, which can reveal too much information of the customer, while the system won't be able to secure the information. Privacy information can be used to embarrass someone in public, steal their money, or find out where someone lives.

Privacy is at risk when sharing information without permission of the owner; surveillance cameras data that are not being used for the right means; abuse of biometric identification, of audit trails, of IP-addresses, of database information, or medical information.

Also, telephone companies retaining telephone records, eavesdropping on telephone calls, banking examining banking records, national security collecting personal information from different sources to profile citizens, companies online collecting personal information about buying preferences of customers via online technology called cookies, and monitoring systems that reveal information about individuals. Even toys are potential problems for privacy, where the toys can record everything happening around them, or connect to Bluetooth devices so children can communicate with parents.

Online personal videos and pictures, on social media, might be reposted without permission. Also, new features on mobile phones such as, location identification via GPS; Automatic files synchronization with external devices; and Web browsers using cookies makes the user information vulnerable for privacy breaches.

Be aware of software in some online app-stores that can be used to hack mobile phones and spy on mobile phone owners. An additional note is the fact that IP addresses are also privacy sensitive.

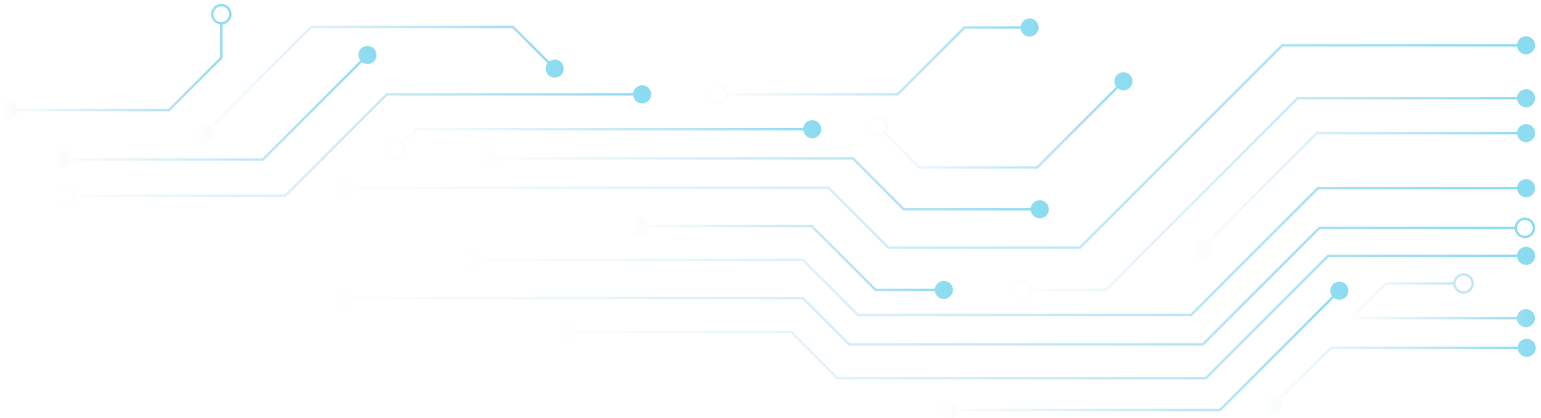

GDPR
esc
control
option
command
alt

There are some solutions for managing privacy risks and guarantee individual's privacy:

1. Vendors should build secure ICT systems with built-in best practices in cyber security measurements to comply with widely accepted privacy principles.
2. Governments should create and implement privacy related laws and regulations.
3. The citizen should protect its own privacy as much as possible when companies and organizations collect personal data. As per May 2018 the GDPR (General Data Protection Regulation) a European law for protection of Privacy of European citizens is effective. However, Curaçao has a privacy act as of October 2010 "AB2010 84", that we all should comply with. Company employee must make sure to protect their own privacy but also the privacy of customers and partners.

BE AWARE OF THE FOLLOWING

- Be aware whenever your personal information is being collected. Inform yourself about how your personal information will be processed, stored and whether your information will be shared.
- Make sure your organization is protecting your privacy, if this one collects your personal information for human resource management administration, tax administration or healthcare.
- Keep your personal matters outside the company's network. The company is not obliged to protect your personal information on the company's network when you are misusing the company's system for personal matters.
- Each piece of information we put on the Internet, stays on the internet. This is also valid for all social media platforms, and it includes also pictures and videos etc.
- The use of personal devices for the office (BYOD), also might mix private and public information.



Bureau
Telecommunicatie en Post

Bureau Telecommunicatie en Post
Beatrixlaan 9, Emmastad
Willemstad - Curaçao

Tel.: +(599-9) 463-1700
Fax: +(599-9) 736-5265
E-mail: gen.affairs@burtel.cw

www.btnp.org