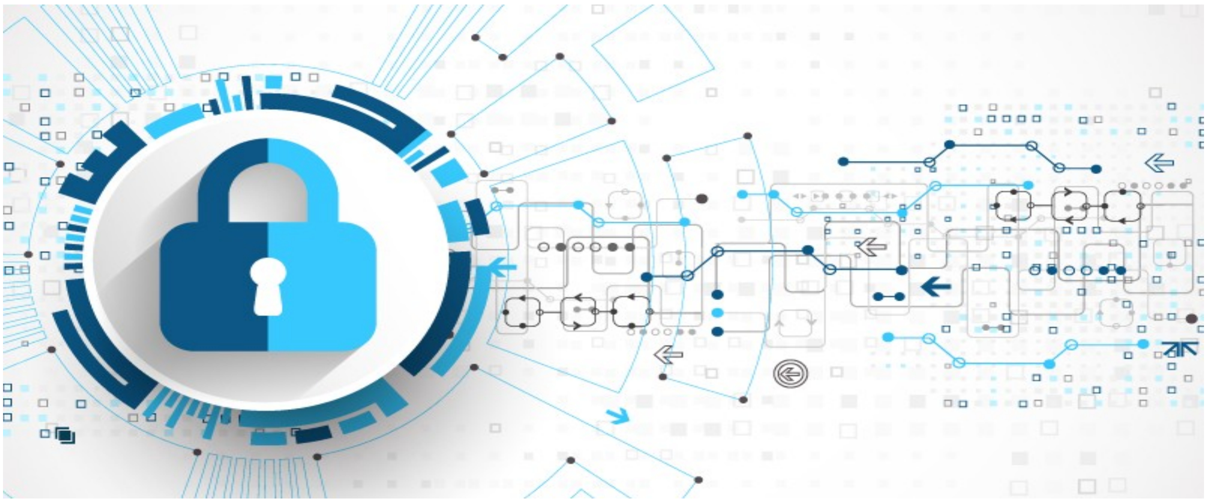
Basic Cyber Security

A guide for all to manage digital Security

January 2019, V1



www.act-security.org

Follow us on Twitter: @ACTSecurity1

01
INTRODUCTION

With the digitalization of our lives, both private and work related, a vast range of new threats have emerged as “soft” threats next to the hard threats in Safety & Security like car accidents, shooting, kidnaps, etc.

In the wake of the introduction of GDPR (General Data Protection Regulation) by 25 May 2018 in the European Union organizations are responsible to safeguard the privacy of and data on staff, clients and relations. Therefore, it’s important that all users of hardware and software are aware of the risks and threats, their responsibility and have to be conscious how to handle information.

These technologies are constantly evolving and something that is valid today might not be tomorrow. It’s important to be always up to date and search for updated information.

Don’t rely on your IT department. The first weak point is the final user.

1.1. To Whom

- For the security management to set up and brief/sensitize/train staff.
- To be read by the staff to know how to use their equipment, email etc.…

Protection of the organization’s asset and information is everyone’s responsibility and not solely of security professionals.

1.2. How to use this handbook

Chapters can be read independently but keep in mind that in a digital ecosystem everything is linked. The slightest flaw can be exploited. It is therefore recommended to take the time to read all the chapters in order but, **first of all, you should do the Self-evaluation of you cyber security**.

See check list in page 27.

This icon link to basic advice for final user.

This icon link to more advance advice for user who want to increase their anonymity.

This manual has been designed to be printed in A5 booklet format

02
PASSWORD MANAGEMENT

02.1 Why a password

With the proliferation of online services (e-mail, merchant sites, document hosting, social networks, etc.) we now have to manage many passwords.

A password is a secret element that only you must know as they condition access to give you services online.

The main risk is related to its use and disclosure to a third party who could misuse it by impersonating you to perform actions on your behalf. The consequences vary depending on the type of service impacted and the objectives of the malicious individuals:

- Compromise personal message on your email.
- Publications of harmful messages or photos on your social networks.
- Data destruction.
- Purchase on online sales sites
- Bank transfer
- Etc.

02.2 Protect your identity

Identity theft can have significant consequences for you and your organization.

Therefore, if you are a victim of identity theft, it is necessary to follow these tips:

GOOD PRACTICES

1 **As part of your professional activity, notify your manager and / or IT security officer.**

2 **File complaints with the police.**

3 **Immediately report the usurpation to the relevant banking, social or administrative services.**

4 **Ask your groups of friends, discussion, etc. to erase harmful messages that do not emanate from you.**

02.3 How can it be stolen -the different types of attack

There is a very large number of possibilities to steal a password but the most common techniques are:

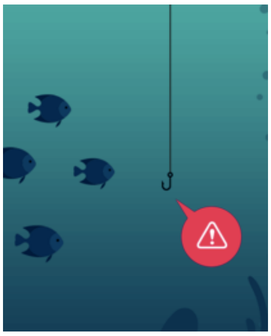
Direct attacks

"Direct" attacks are those by which an attacker tries to recover your login and password to log in your place. The list is long but here are some of the techniques.

- ***Brute force attack*** is the simplest direct attack. It consists, using software, to test all passwords (including special characters) possible one by one until you reach the right one.
- ***Distributed Attack*** consists of **distributing the workload of the software between multiple computers**. Thus, several infected computers can work at the same time to identify the password, reducing the identification time***.***
- ***Proximity attack*** is a **direct look at your password** when typing, or when it is written on a post-it or chalkboard in your office.
- ***Key logger,*** are **software installed on your computer that will record all keystrokes on your keyboard** and transmit them over the Internet to the person who controls the program. These programs are easily available on the Internet, for free or for a few dollars depending on their complexity.

Indirect attacks

Unlike direct attacks that steal your passwords on your desktops or when typing you, indirect attacks use the trick to trap you and recover your authentication information without your knowledge.

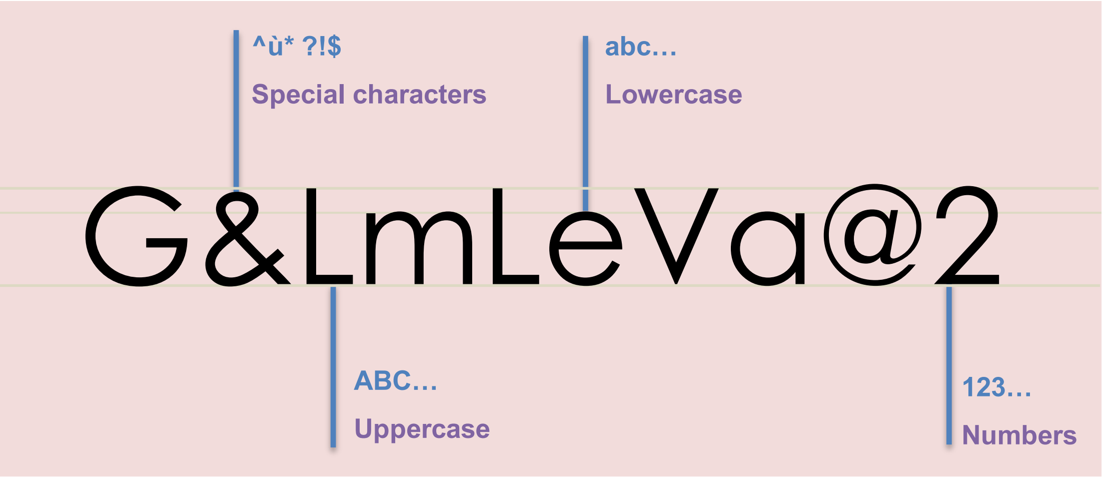


- ***Phishing*** is to **send an email prompting to click on a web link to solve a problem**. In reality the link leads to a fraudulent site, sometimes very well done, which will push you to register your identification elements which will then be registered.
- ***Reuse password.*** Many users today still use the same password for a number of sites. **Hackers attack low-security sites such as amateur forums or buy lists of passwords from pirated sites on parallel markets and then reuse them on more profitable sites**, such as websites. banking or courier services.

02.4 How to choose a good password

What is a good password?

A good password, which is called strong, must be difficult to discover by an attacker in a reasonable time and with the help of automated tools.



Golden rules to create a password

1. At least **10 characters.**
2. Use a **varied character set** (not just letters and numbers but uppercase, lowercase, numeric, special).
3. **Avoid reporting to your identity** (surname, first name, date of birth, first name parents / children, etc.)
4. **Not related to the name of the service** for which it is used (pwdHotmail, NameOfmyNGO).
5. **Ban dictionary words**.

A password is personal, nobody or any site will ask you. If this is the case then it is a fraudulent attempt.

How to memorize a good password?

How to retain a password such as "Pa_ (uYç! &" without needing to write it somewhere or reset it each time?

1. Define a phrase consisting of four random words and then concatenate them.

   Exemple. Screen:Sun:window:currant

2. Use phonetics, that is, remember the sounds of each syllable to make a sentence easy to remember.

   Exemple. J'ai acheté huit CD pour 100 dollars cet après-midi

   Ght8cd%$7aM

Here is a website that will allow you to determine how long it would take a software to discover your password:

https://howsecureismypassword.net/

How to protect your password

- Use different passwords to authenticate with separate systems
- Do not type your passwords on a machine you do not trust
- Do not store your passwords in plain text on your computer or on a post-it
- Do not send your passwords by email, SMS, traveling pigeon, etc.
- Change your passwords immediately to the slightest suspicion of leaking
- Delete service emails that send the password and / or login when registering
- Change the default passwords for all systems / accounts as soon as possible
- Do not use a simple expression like "password" and / or series of numbers and letters

GOOD PRACTICES

For sensitive data (banks, private correspondence, medical, etc.) it is recommended to configure your software and browsers so that they **do not remember your passwords**.

You should **use a Password Manager** that will allow you to manage different password for different website.

www.enpass.io

02.5 How to securely share a password within a team

Managing passwords within a team is a recurring problem. It is not always possible to have unique passwords for each person (for example, the administrator password for a database). It may also be necessary to send a temporary password (for example, Alice creates an account for Bob asking him to change his password).

Many organizations use unspoken practices (unscrambled e-mail, shared files) to exchange passwords that are common to multiple users, undermining their privacy.

Many existing password management solutions focus on the personal needs of their users. Passbolt was designed to meet the needs of a team in small and medium organizations. Moreover, passbolt is completely free.

Passbolt can also help administrators set up rules for rotating, auditing, and replacing passwords, for example, when an employee leaves an organization. Passbolt helps end users to use strong and unique passwords.

https://www.passbolt.com/

03
COMPUTER SAFETY

03.1 Software and update

Ignoring a security update makes your workstation (or phone) vulnerable to a potentially public vulnerability known to hackers. It is therefore necessary to **carry out the updates proposed by the publishers as soon as they are published**.

CAUTION: Be aware of fake update notifications because it can be a trap set by attackers to get malware installed. (Via fake advertisements or alerts).

GOOD PRACTICES

1. **Enable automatic updates**.
2. Download only **software and updates from trusted sources** (publisher's site).
3. If the software asks you to access too much personal information (your contacts or SMS on your phone for example) then **find another solution and do not install**

03.2 Removable devices and USB

Removable devices and especially USBs all have a firmware that can be modified to perform various attacks. These elements can therefore behave like a virus and infect your computer in a completely transparent way.

Putting personal information and mixing pros and personal uses pose a risk of cross infection for your organization and yourself.

GOOD PRACTICES

1. **Never connect** to your computer a **removable device from a dubious source** (found in the street, offered has a gift etc.)
2. **Separate uses** (work and personal).
3. Do **not put sensitive information** (or encrypt it).

03.3 Data Management

Governments usually have the means to monitor organizations' phone calls, Internet activity, Facebook, Twitter, etc. as well as hack your computer hard drives.

Criminal organizations will also perceive NGOs as wealthy, given the vehicles, laptops, satellite phones they often use, as well as publicly announced donor funding levels.

All of this makes aid agencies vulnerable to information security risks and this is why we have to properly manage the security of our data by encrypting files and email, managing their classification and securely backup data.

BE AWARE THAT IN SOME COUNTRY ENCRYPTION IS ILLEGAL.
PLEASE CHECK YOUR LOCAL RULE OF LAW

1. How do we encrypt files?

Why encrypt documents and directories?

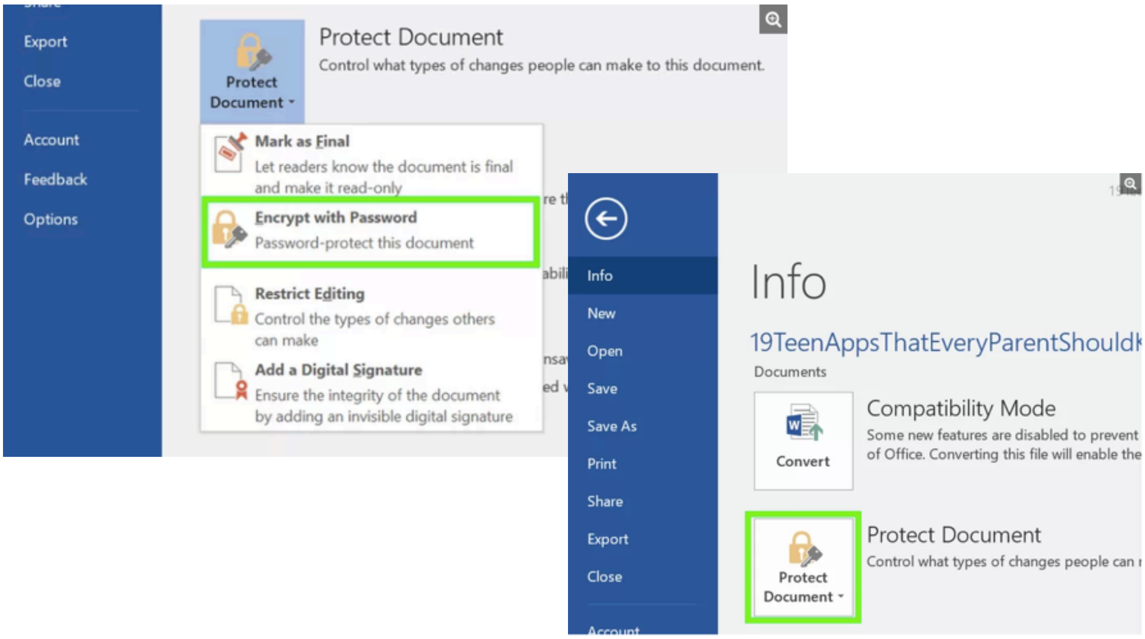
Encrypt a folder allows you to block unwanted access to your personal files (photos, videos, work documents and emails).

Moreover, encryption is a way of scrambling using an algorithm (mathematical formulas), which is difficult to decipher. In other words, a key without which no one can open your files protects your files.

Method 1: Encrypt a Microsoft Office document

When your document is open (Excel, word, power point etc.)

- **Click on File > Protect workbook/document >Encrypt with password**



Protect Document
Control what types of changes people can make to this document.

Mark as Final
Let readers know the document is final and make it read-only

Encrypt with Password
Password-protect this document

Restrict Editing
Control the types of changes others can make

Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature

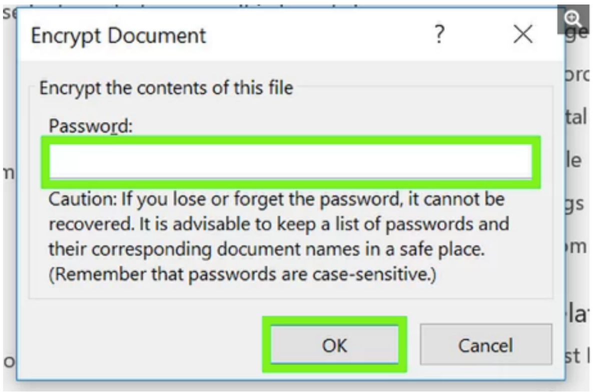
Info

19TeenAppsThatEveryParentShouldk
Documents

Compatibility Mode
Some new features are disabled to prevent of Office. Converting this file will enable the

Protect Document
Control what types of changes people can r

- **Enter a password for the file.** You'll be prompted to re-enter the same password, then click OK. After you exit this file, you'll have to enter the same password to reopen it



Encrypt Document

Encrypt the contents of this file

Password:

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

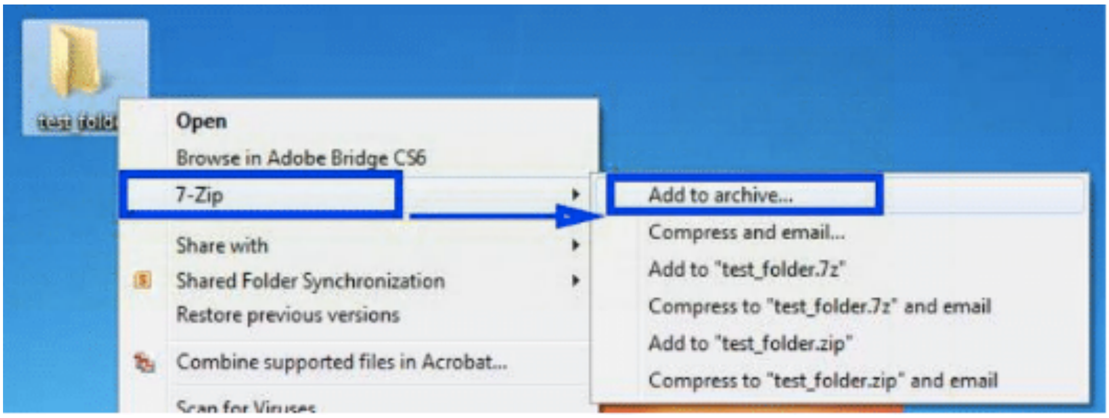
Method 2: Encrypt a document or folder with 7-Zip

7-Zip is software that can compress one or more documents and encrypt them. It is free, downloadable on http://www.7-Zip.org, available in several languages and freely redistributable.

Once the software is installed, please follow following steps to encrypt a file or folder.

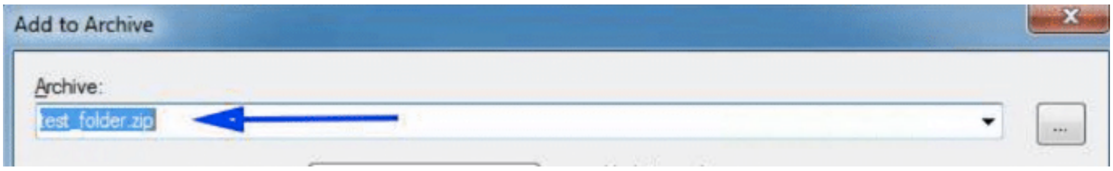
Step 1: Right click on the file / folder to be encrypted**.**

Step 2: Select "7-Zip" then **"Add to archive..."**



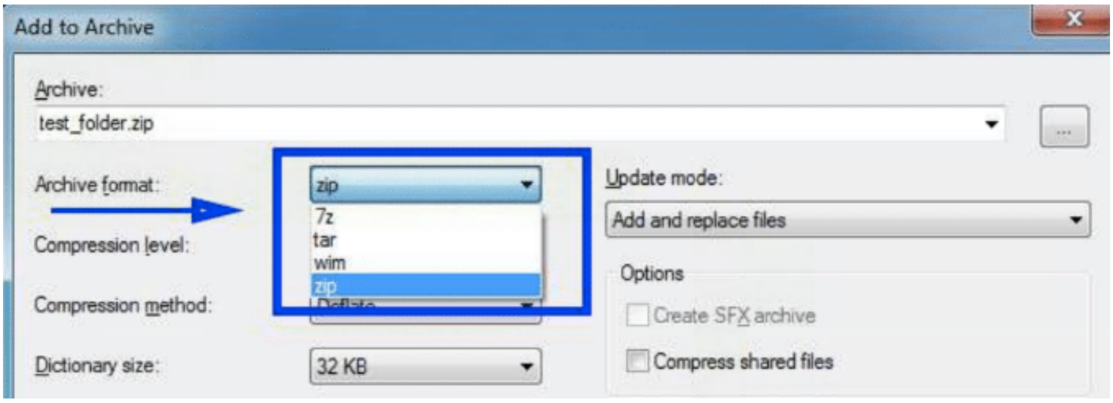
test fold
Open
Browse in Adobe Bridge CS6
7-Zip
Share with
Shared Folder Synchronization
Restore previous versions
Combine supported files in Acrobat...
Scan for Viruses
Add to archive...
Compress and email...
Add to "test_folder.7z"
Compress to "test_folder.7z" and email
Add to "test_folder.zip"
Compress to "test_folder.zip" and email

Step 3: In the Add to Archive window change the name of the archive you wish to create.


Add to Archive

Archive: test_folder.zip

Step 4: Change the Archive format **to "Zip".**


Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level:

Compression method: Deflate

Dictionary size: 32 KB

Update mode: Add and replace files

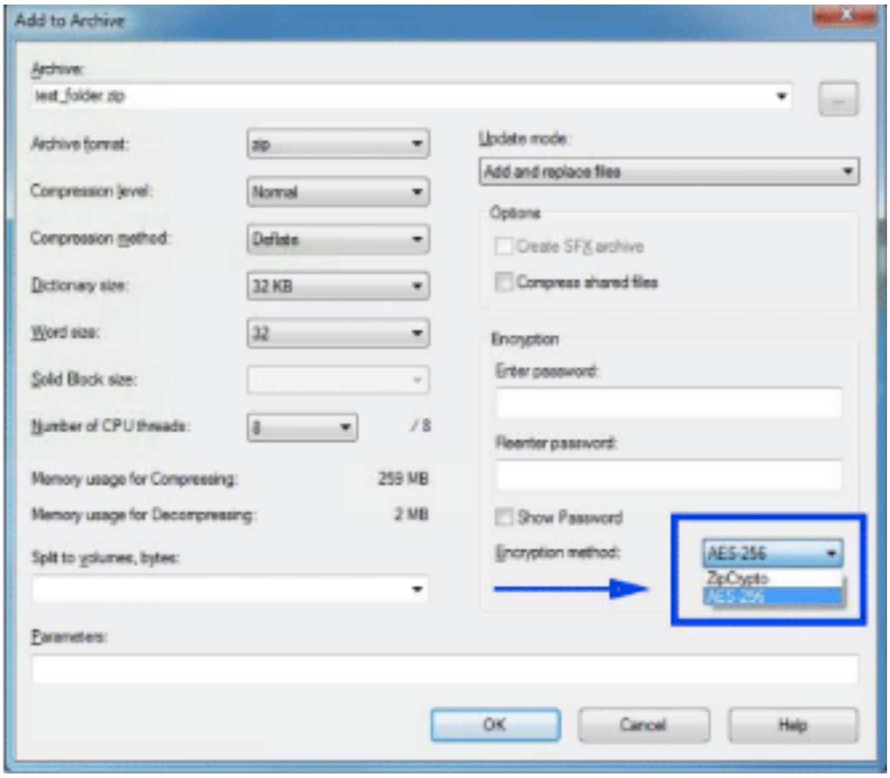
Options

□ Create SFX archive

□ Compress shared files

Step 5: Change the Encryption Method to **"AES-256".**

It is strongly recommended to use AES-256 compare to ZipCrypto to protect sensitive and confidential data, even though this mean the recipient will have to install 7-Zip as well.


Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

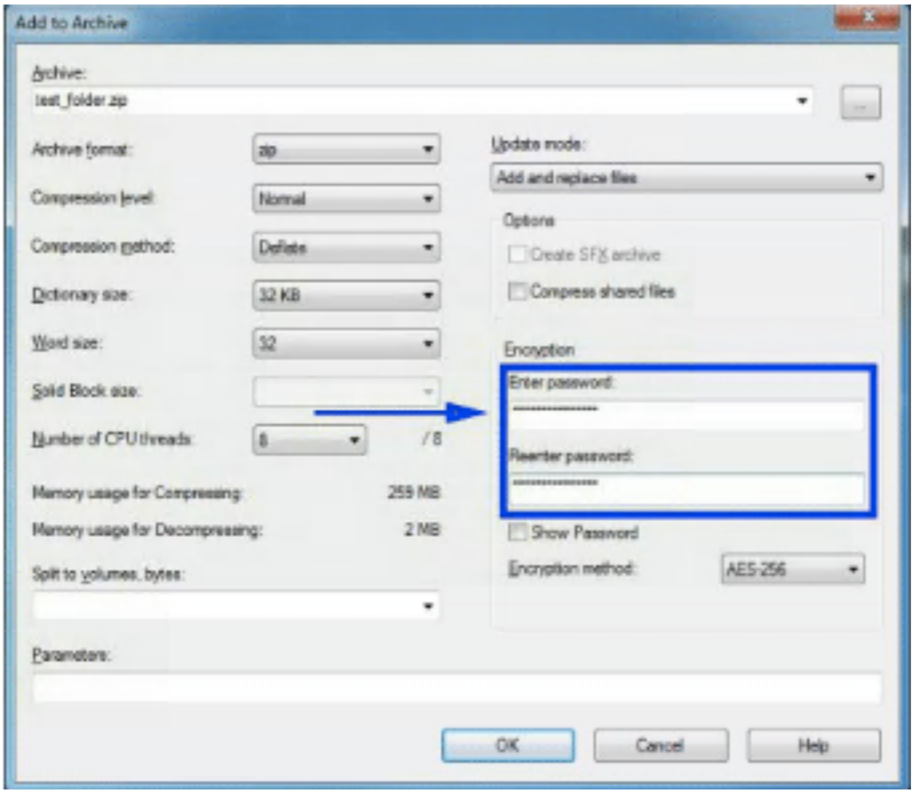
Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

Step 6: Enter a Password. See Chapter 2 on how to choose a strong one.


Add to Archive

Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

Enter password: ****************

Reenter password: ****************

□ Show Password

Encryption method: AES-256

Step 7: Select "Ok" to create the encrypted archive file. The new archive file will be located in the same folder as the original.

GOOD PRACTICE

- Anything can be decrypted if you're targeted by a savvy enough, or well-financed foe. You might want to **find a paid solution if your files are truly sensitive**.
- Files encrypted using the above methods can still be deleted, so you might want **to have a backup on a secondary location.**
- If you lose your passwords, you've lost your files forever. So, again, **keep an unencrypted backup on a physical drive somewhere safe** where it won't be found.

Method 3: Encrypt your computer hard drive or external storage device

Vera Crypt is free and open source software that will protect your files by encrypting them with a passphrase. It allows you to encrypt your computer hard drive, a USB key or your external storage device use for back up

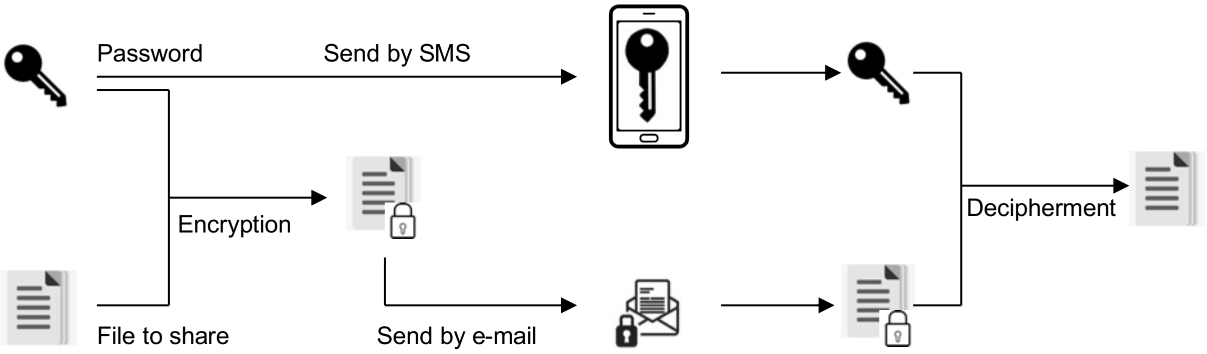
To go further on the encryption of your hard drive or any external storage

Follow the step-by-step process detail here:

https://securityinabox.org/en/guide/veracrypt/windows/

2. How to securely share files

Once the file have been encrypt send it in one email and the password through other means (e.g. through Skype, WhatsApp or phone call).



Once you have encrypted your files you can now share them securely.

To read them, the recipient must know the password used as an encryption key. It will therefore be necessary to send him.

To ensure the confidentiality of the file it will be necessary to share it by a channel (ex: email) and your password by another one (ex: WhatsApp).

Thus, if one of the channels is compromised it will be impossible to know the contents of the file because it or the password will be missing to decrypt it.

Data classification[1]

The sharing of some information may be considered an obligation for all organization and a matter of policy.

It is important that an organization decides **what information they are willing to share, to whom and for what purpose.** The below table provides an example of how the sensitiveness of information may affect the access level.

Confidential	Confidential information has significant value for the organization, and unauthorized disclosure or dissemination of it could result in severe reputational damage or adverse impact on the organization's operations. ✓ Only those who need access explicitly should be granted it, and only to the least degree necessary (the 'need to know' and 'least privilege' principles). ✓ When held outside the organization's offices such as on laptops, tablets or phones, confidential information should be protected behind explicit logons and possibly encryption devices and/or encrypted email platforms.
Restricted	Disclosure or dissemination of this information is not intended, and may incur impact on people's lives, some negative publicity or limited reputational damage or potential financial loses to the organization. ✓ Restricted information is subject to controls on access, such as only allowing valid logons from a small group of staff. ✓ Should be held in such a manner that prevents unauthorized access i.e. on a system that requires a valid and appropriate user to log in before access is granted.
Internal Use	The dissemination of the information to the relevant stakeholders ensure good functioning and responses, internally to the organization or working group. Its release will not cause any damage to the organization or its staff but is considered as undesirable. ✓ Internal Use information can be disclosed or disseminated to appropriate members of the organization, partners and other individuals, as appropriate by information owners.
Public	The dissemination of the information through news media and other channels is not posing any risk to the organization or its staff, and its release is considered desirable or non- objectionable at least.

[1] From the « *Security Incident Information Handbook* » (SIM), developed by RedR UK, Insecurity Insight and EISF.

	✓ Public information can be disclosed or disseminated without any restrictions on content. ✓ Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules.

How to back up data

Definition

A backup of your data allows you to keep a copy of your actual data by saving it in another location.

Why it is important

By doing this, if your main drive where all your data is lost, destroyed or not working anymore (through a technical issue or virus, a user error, a theft of a device...), you will be able to recover it from the other location.

BACK UP	
Purpose	**Restoring data if needed**
Data concerned	**A copy of all immediate data needed for everyday operations**
When to do it	**On a regular basis**
Where to do it	**On an external Hard Drive**
Is their sensible information	**Encrypt your hard drive**

How do to it

How to back-up your data will depend on the type of data and the device on which the data is stored.

Your backups should preferably be stored outside of the offices to prevent the destruction of the original data from being accompanied by the destruction of the backup copy in case of fire or flood, or the backup copy to be stolen at the same time as the computer containing the original data.

The choice of location should not be taken lightly to prevent the data from being stolen by hackers.

GOOD PRACTICE

- Back-up device can get lost or stolen. Encrypt it using the software VeraCrypt as describe on page 15.

How to destroy sensitive information

When deleting a file the system simply indicates that the file storage location is reusable.

Other data will be rewritten over time ... maybe the next day or maybe in a year. When you delete a file, even after you empty the recycle bin, the contents of that file remain on your hard drive and can be recovered by anyone who has the right tools.

Moreover, with professional software it is sometimes possible to find data even after several writing cycles. It is therefore necessary for the extremely sensitive data to perform erasure (this specific process is call wiping) by rewriting the file via a dedicated tool to ensure the actual destruction of data.

To go further in the secure destruction of its files

- **Periodically use CCleaner to clean temporary files.**
- **Periodically use Eraser to clean space on your hard drives, USB memory sticks, and any other storage devices.**

https://securityinabox.org/en/guide/eraser/windows/

04
INTERNET SECURITY

One of the most common misconceptions is that computer attacks only affect state administrations and large corporations.

SPAM, malware, spyware, keylogger, ransomware all these threats (and many others) can be received by email, downloaded on the web or shared via USB sticks. The risks are many!

Fraudulent use of your credit card, identity, blackmail broadcast of a compromising video, but also use of your data to retaliate on your NGO, government control etc.

It is therefore a question of protecting oneself by adopting a behavior and by setting up and a set of actions when you use the internet tool.

04.1 Files from the internet

The files we download and share on the Internet are the source of many cyber attacks.

The most exploited formats by hackers are *Microsoft PDF* or *.EXE* or *.DOC* or *(X) / XLS (X)* type files, simply because they are the most used.

Someone who is malicious will try to exploit these formats to incite a user to innocently open a file. It will be able to execute malicious code and contaminate your computer without you understanding why you cannot open the file.

GOOD PRACTICES

- **Disable automatic execution** of removable devices.
- Do not open files that come **from unreliable sources.**
- **Be aware of executable files (.exe, dmg)**
- Download software (free or paid) **only from the publisher's website (**with a green tick next to it)
- **Always show the file extension**

Windows 10

Explorateur de fichiers > Affichage > Extensions de noms de fichiers

04.2 Web browsing

Websites are the most common source of malware infection, so accessing them securely is vital.

Do not give personal and confidential information (your personal details, your bank details, etc.) on a merchant site or a banking site, without first checking that the site is secured. It should use an electronic certificate that guarantees that the site is authentic, and that will serve to protect the confidentiality of information exchanged.

For this, there are two pieces of information displayed by the browser that must be checked:

1. The URL of the site must begin with "https: //" and the site name must match the user's expectation;
2. A small closed padlock must appear to the right of the site address, or at the bottom right of the status bar (depending on the version and type of your browser); it symbolizes a secure connection. By clicking on it, you can display the electronic certificate of the site, and view the name of the organization.

However, it is always possible for an attacker to intervene upstream (on your machine) or downstream (on the site consulted or by referring you to a fraudulent site with a very similar name) in order to obtain sensitive information.

GOOD PRACTICE

The overwhelming majority of malware and spyware infections originate from web pages.

It is important that you always consider whether it is safe to visit unknown websites, particularly those that are sent to you by email.

Before you decide to before opening a web page you are not sure about, use, we recommend that you scan the web address using the following URL scanners (add it to your bookmark):

www.virustotal.com

Navigate with a browser up to date

What is true for an operating system, is also true for the software that is installed there. Before using any browser, make sure that it is up to date as soon as possible. The most recent browsers **all offer an automatic update feature. Check in the settings that this one is activated**.

Message pop-up

Beware of pop-up windows: they are often the occasion to broadcast commercials but can sometimes **carry a perfectly wrong alarmist message ("your computer is infected!"). Click on the links of these windows until after careful reflection**.

Conversely, do not fall into the panel of enticing promises. The most primary instincts are often solicited to get the user to visit a site whose content can be dangerous.

Password

Do not save passwords in your browser to access your favorite websites, especially if they are e-commerce or banking sites (PayPal included). The security of these identifiers, in case of viral intrusion, is not guaranteed.

See page 5 for more information.

To go further on the security of your browser and the ability to navigate in the most anonymous way possible

https://securityinabox.org/en/guide/firefox/windows/

04.3 E-mail

Best practices to better understand e-mail:

GOOD PRACTICE

- **Reinforce the password** of your mailbox (use a password safe).
- **Do not consider the sender's e-mail address as a reliable** criterion as it can easily be misused.
- **Never give confidential information** by mail or telephone
- **Do not open attachments without scanning it** with your antivirus, even if it is a trusted person who sends it to you.
- **Do not click on the links in the emails** (move your mouse over it and look at the corresponding address that appears in the status bar at the bottom left of your browser).

Switching to a more secure email account

Few webmail providers offer very strong access to your email. Yahoo and Hotmail, for instance, provide a secure connection only while you log in, to protect your password, but your messages themselves are sent and received insecurely. In addition, Yahoo, Hotmail and some other free webmail providers insert the IP address of the computer you are using into all of the messages you send.

But be careful, Gmail is known for potentially allowing government to get access to your email if requested.

If you need an extra layer of confidentiality please read the section below.

To go further on the security of his e-mails

- **Install Thunderbird email client and the add-on [ProtonMail](#) or [Enigmail](#) (invitation requested).**

https://securityinabox.org/en/guide/thunderbird/windows/

04.4 Social Network

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. The biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common.

So for this:

- Pay attention to settings and information that you share.
- Only invite and accept people you know.
- Determine where you make your information visible and check what other users see in your profile.
- Do not share information about your professional activities.
- Only post picture on social media after you left the place

Always ask yourselves the questions:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?

- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I'm connected?

There is also a very large number of scams that can be easily avoided.

- Be cautious about promotional videos with sensational titles.
- Be careful with publications that require an addition as a friend or a thumbs up before you can access more content

04.5 Public Wi-Fi

If free Wi-Fi networks are now very accessible, they pose a risk to personal information stored on a smartphone, tablet or laptop.

The misuse of a public Wi-Fi network may allow an attacker to simply recover the data you exchange with an e-commerce site or to obtain your bank details and access credentials to your account.

GOOD PRACTICE

There are two simple rules to follow:

1. **Avoid connecting to unknown or untrusted wireless networks.**
2. **Avoid using public Wi-Fi to transmit sensitive data.**

04.6 Your organization Wi-Fi

A poorly secured Wi-Fi can allow people to intercept your data but also to use the Wi-Fi connection without your knowledge to perform malicious operations.

- Check that your terminal has the **WPA2 decryption protocol** and enable it. Otherwise, use the WPA-AES version (never use breakable WEP decryption in minutes).
- **Change the default login key** (which is often displayed on the label of your Internet access point) with a strong password.
- **Give your network an anonymous name** so that it does not identify you with your organization.
- **Use wire connections as much as possible**, faster and more secure.

05
SMARTPHONE SECURITY

The way the mobile networks operate, and their infrastructure, are fundamentally different from how the Internet works. This creates additional security challenges, and risks for users' privacy and the integrity of their information and communications. Mobile phone providers (so government as well) have access to all your voice and text communications.

It is important to start with the understanding that mobile phones are inherently insecure:

- Information sent from a mobile phone is vulnerable.
- Information stored on mobile phones is vulnerable.
- Phones are designed to give out information about their location.

GOOD PRACTICE

- **Set a strong PIN**. Always use your phone's security lock codes and change these from the default factory settings.
- **Do not accept and install unknown and unverified programmes** on your phone that originate from an unwanted and unexpected source. They may contain viruses, malicious software or spying programmes. Android user, only download apps from the Google Play Store.
- **Be wary when connecting to Wi-Fi access points** that don't provide passwords, just as you would when using your computer and connecting to Wi-Fi access points. The mobile phone is essentially like a computer and thus shares the vulnerabilities and insecurities that affect computers and the Internet. Favour 3G / 4G connections.
- **Check which applications you are installing** and what they are requesting in terms of access. Ex: If you install a flashlight application and it asks you to have access to your GPS coordinates and SMS data then do not install it and look for another one!
- **Pay attention to the data you share with your phone.** (> Settings> privacy and check what apps have access to).

To go further on the encryption of your smart phone communication

Install Signal App. Signal messages and calls are always end-to-end encrypted

06 COMMON SCAM

The most common scam happens when you:

- Check your email addresses
- Access your social media networks

06.1 Phishing email scams

More than one third of all security incidents start with phishing emails or malicious attachments.

Phishing scams are based on communication made via email or on social networks. In many cases, cyber criminals will send users messages/emails by **trying to trick them into providing them valuable and sensitive data** (login credentials – from bank account, social network, work account, cloud storage) that can prove to be valuable for them.

This way, they'll use social engineering techniques **by convincing you to click on a specific (and) malicious link** and access a website that looks legit, but it's actually controlled by them. You will be redirect to a fake login access page that resembles the real website. If you're not paying attention, **you might end up giving your login credentials and other personal information**.

GOOD PRACTICE

1. First thing to check: the sender's email address**.** Look at the email header**. Does the sender's email address match the name and the domain?**
2. **Hover your mouse over the links** in the email message in order to check them BEFORE clicking on them.
3. **Look out for attachments; think twice before to open it.**
4. They ask you to send them or verify personal information via email. **If you have doubt look for official phone number of the company** and ask them if they sent the email.

06.2 Facebook security

Few tips to help you stay away from Facebook online scams:

- Do not accept friend requests from people you don’t know
- Do not share your password with others
- When log in, use two-factor authentication
- Avoid connecting to public and free Wi-Fi networks
- Keep your browser and apps updated

GOOD PRACTICE

To keep your Facebook account safe: open Facebook in your browser and go to **Settings > Security and Login > Setting Up Extra Security.**

From there:

1. **Turn on login alerts** so that you receive notifications when your account is logged into. This helps you catch a hacker early, before any major damage is done.
2. **Enable two-factor authentication**, then choose an extra layer of security from the list.
3. Choose your trusted contacts and add a few close friends or family members that can help you unlock your account if it ever becomes hacked.

ANNEX: CHECK-LIST FOR A SECURE DIGITAL ECO SYSTEM

Topic	Strong	Medium	Weak	Related Chapter and page
My password is of at least 10 characters				**What is a good password?** Page 7
My password are saved in my browser				**How to protect your password** Page 8
I know how to share a password with my team.				**How to securely share a password within a team** Page 9
I know how to manage software update.				**Software and update:** Page 27
I'm following strict removable device policy				**Removable device and USB** Page 10
I encrypt sensitive files				**How do we encrypt files?** Page 11
I operate to a classification of my Data				**Data classification** Page 16
I'm regularly and safely backing up data				**How to back up data** Page 17
My web browser is up to date and allow me to anonymously surf on the internet				**Web browsing** Page 20
I know the basic email security management				**Email** Page 21
I know how to send encrypted email				**Switching to a more secure email account** Page 22
I recently checked the vulnerability linked to my social network account				**Social network** Page 25
I know the 2 rules to properly use a public Wi-Fi				**Public WI-FI** Page 23

I know that my Wi-Fi network is on WPA2				**Your organisation Wi-Fi** Page 23
There is a strong PIN to connect to my mobile phone.				**Smartphone security** Page 24
I know the permissions granted to the applications installed on my phone.				**Smartphone security** Page 24
If my computer/phone get stolen I can reach 27/7 my IT dep.				**Contact your IT dep.**
I'm aware (and following) my NGO IT policy				**Contact your IT dep.**

NOTE: