**Information Security**

**MANAGING INFORMATION**

*BASIC*

**1. Keep what you need**

The most basic rule for managing information securely is that any information that could put people at risk should always be compartmentalised and kept ‘need to know’. This means that only those people who really need that piece of information to operate should be given it. For example, if a team is working with a high-risk source, only the source’s direct contact within the team should have his or her real name and details – the rest of the team can operate using a code name. This reduces the risk for both the source and those other members of the team.

If there is not a good reason to keep a piece of sensitive information then you should simply delete it (see the Safely Deleting lesson).

**2. Threat Modelling**

There is no single solution for keeping your information safe. Managing your information securely isn’t about which tools you use; it’s about understanding the threats you face and how you can counter those threats. To become more secure, you should figure out what you need to protect, and whom you need to protect it from. Threats can change depending on where you’re located, what you’re doing, and whom you’re working with. The easiest way to figure out what solutions are best for you is to carry out a threat modelling assessment.

**3. Assessment questions**

When carrying out an assessment, there are five main questions you should ask yourself:

1. **What do you want to protect?**

What information could put you, your work or others at risk if were public? This is often the kind of information kept in your emails, contact lists, messages and files. It might relate to a specific sensitive campaign you are working on.

1. **Who do you want to protect it from?**

This could be any person or entity that poses a threat against an your or your work, also known as an adversary. Think about who would have a motive in reading or deleting your information or disrupting your work. Examples could be a government, a company you are exposing, your boss, or a hacker.

1. **How likely is it that you will need to protect it?**

It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. Calculating risk means figuring out the chance that a threat might actually occur – how likely is it that a threat would be carried out? You also need to think about the capability of potential attackers. For example, your mobile phone provider has access to all of your phone records and therefore has the capability to use or share that data. A hacker on an open Wi-Fi network can access your unencrypted communications. A government might have stronger capabilities.

1. **How bad are the consequences if you fail?**

The motives of adversaries differ widely, as do their attacks. A company trying to prevent the spread of a video showing their illegal activity may simply want to delete the video, whereas a government may wish to gain access to the names/details of activists it sees as a threat to the state in order to arrest or harass them.

1. **How much trouble are you willing to go through in order to try to prevent those?**

This means figuring out which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about. Many people find certain threats unacceptable no matter what the risk, because the presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

**4. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Safely Deleting lesson*

*FURTHER READING*

* [*EFF - Threat modelling*](https://ssd.eff.org/en/module/introduction-threat-modeling)

***Managing Information Basic Checklist***

* ***Implement ‘need to know’ policy***
* ***Delete any unnecessary sensitive information***
* ***Make a list of information that you keep, where it’s kept, who has access to it, and what stops others from accessing it***
* ***Make a list of who might want to get a hold of your information***
* ***Note what your adversary might want to do with your information***
* ***Note the likelihood of your adversaries attacking***
* ***Note the capability of your adversaries to attack***
* ***Note what the consequences are if the attack succeeds***
* ***Note what you are you willing to go through in order to try to prevent them***

**MALWARE**

*BASIC*

**1. What is malware?**

Malware, short for "malicious software," is software that is used to harm computer users. It can do things like gather information, impersonate a user, gain access to other computers, or stop a computer from working. It could do this by allowing an attacker to record from a webcam and microphone, disabling anti-virus programs, recording keystrokes, copying emails and other documents, stealing passwords, and more. Most malware is criminal and is often used to obtain banking information or other valuable information. However, it is also used by governments, law enforcement agencies, and even private citizens to spy on users.

**2. Is my computer infected?**

**Anti-virus software**

You should always use anti-virus software on your computer and your smartphone, which are easily available to buy and download. Avast is an easy to use anti-virus program for Windows. Clam Win is a good open source alternative. Anti-virus software can be quite effective at combatting cheap, “non targeted” malware that might be used by criminals against hundreds of targets. However such software is usually ineffective against targeted attacks, such as ones carried out by governments against.

**How can I tell if my computer is compromised?**

Malware is very difficult to detect. Scanners such as Spybot or [Malwarebytes](https://www.malwarebytes.org/) can detect and protect against some malware threats and are useful to use.

While most malware avoids detection by software, it is still sometimes possible to find indicators of it on your computer. For example, services will sometimes send you a warning email if they believe your account has been targeted, you may notice a light indicating that your webcam is turned on when you have not activated it yourself, or your settings have been altered to send copies of your emails to an unfamiliar email address.

**3. How can attackers use malware to target me?**

The most common method of attack is to trick you into installing the malware yourself. There are many ways they try to do this.

* They may disguise the malware as a link to a website, a document, a software update, or even a program designed to help secure your computer.
* You may be targeted via email (which may look as if it’s coming from someone you know), via a message on Skype or Twitter, or even via a link posted to your Facebook page.
* You can also infect your computer by connecting infected hardware, like a USB key given to you or found near your office, or a phone connected to charge.

The more targeted the attack the more they’ll try to make it look like something you want to open. For example, in Syria, pro-Assad hackers targeted members of the opposition with malware hidden in fake revolutionary documents and a fake anti-hacking tool. And in Morocco, activists were targeted with malware hidden in a document made to look as if it had been sent by an Al-Jazeera reporter, promising information about a political scandal.

There is also the possibility of someone gaining physical access to your computer to install malware themselves. You can read more about preventing against such attacks in the – Office lesson.

**4. How can I avoid getting infected?**

* Always make sure you are running the latest version of your software and downloading the latest security patches. Only the latest updates have the latest protections. It is a common belief that if you are running an unregistered copy of Windows, you cannot or should not accept security updates. This is not true. Always update. [Secunia PSI](https://secunia.com/products/consumer/psi/sys_req/) for Windows is a free tool that will check to make sure your software is up to date.
* Only download software from official sites.
* Avoid open opening suspicious attachments (anything from someone you don’t know) or clicking on suspicious links (any links you didn’t request)
* If you are using Gmail, open unusual attachments in Google Drive rather than downloading them.
* Double check the sender’s email address if you get an email with an attachment or link you weren’t expecting, even if the email appears to be written by a friend or colleague. If something seems odd or their tone is unusual, it doesn’t hurt to email the friend to check they sent it and mention it to colleagues.
* Stay alert when browsing websites. Watch for browser windows that appear automatically, and read them carefully. When in doubt, you should close 'pop up windows' by clicking the **X** in the upper corner, rather than by clicking **Cancel**.
* Disconnect your computer from the Internet when you are not using it and shut it down completely overnight

**5. What should I do if I find malware?**

* The first thing you should do if you find malware on your computer is *unplug your computer from the Internet and stop using it immediately.*Every keystroke you make may be being sent to an attacker.
* Log into a computer you believe is safe and *change your passwords;*every password that you typed on your computer while it was infected should now be considered to be compromised.
* You may wish to reinstall the operating system (eg Windows, Android, IOS) on your computer in order to remove the malware. This will remove most malware, but some especially sophisticated malware may persist.
* If you can, take your computer to a security expert, who may be able to discover more details about the malware.
* If you have some idea of when your computer was infected, you may reinstall files from before that date. *Reinstalling files from after the date of infection may re-infect your computer.*

**6. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on how to protect yourself against targeted malware attacks.**

*FURTHER READING*

* [*EFF - How do I protect myself against malware*](https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware)
* [*Security in a Box - Chapter 1, Malware*](https://securityinabox.org/chapter-1)

***Malware Basic Checklist***

* ***Protect your computer***
  + ***Install antivirus on all your devices***
  + ***Install a malware scanner on all your devices***
  + ***Look out for indicators of malware***
  + ***Keep your software updated***
  + ***Only download from official sites***
  + ***Avoid opening suspicious attachments***
  + ***Open unusual attachments in Google Drive***
  + ***Double check senders email address for unexpected attachments***
  + ***Close pop-up windows in the corner***
  + ***Use a platform like Ubuntu or Chrome***
* ***If you find malware***
* ***Unplug your computer***
* ***Stop using your computer***
* ***Log into a safe computer and change all your passwords***
* ***Reinstall operating system***
* ***Take your computer to a security expert***
* ***Only reinstall files from before date of infection***

*ADVANCED*

**1. Tips on using anti-virus software effectively**

The beginner lesson gave a run through of useful anti-virus software such as Avast or Clam Win and anti-malware software such as Spybot or Malwarebytes. There are a few ways in which you can make sure you get the most out of your software.

* Do not run two anti-virus programs at the same time, as this might cause your computer to run extremely slowly or to crash. Uninstall one before installing another. However anti-malware software is designed to work alongside anti-virus software.
* Make sure that your anti-virus program updates itself regularly. Without updates it can quickly become ineffective. All of the software recommended here supports free updating.
* Enable your anti-virus software's 'always on' virus-detection feature if it has one. It may also be called 'Realtime Protection,' 'Resident Protection,' or something similar.
* Scan all of the files on your computer regularly. You don't have to do this every day but you should do it from time to time. How often may depend on the circumstances. Have you connected your computer to unknown networks recently? With whom have you been sharing USB memory sticks? Do you frequently receive strange attachments by email? Has someone else in your home or office recently had virus problems? Tools such as Avast can do this for you.

**2. Preventing virus or spyware infection**

* If you need to open a file from someone you don’t know well, you should save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the program's File menu to open the attachment manually, rather than double-clicking the file or allowing your email program to open it automatically, you are less likely to contract a virus.
* Hover over URLs and hyperlinks to check where they lead. If you're unsure about a URL, check it at [VirusTotal](https://www.virustotal.com/#url).
* Before inserting removable media, such as CDs or USB sticks, into your computer, you should disable your operating system's 'AutoPlay' feature. (This is usually found under the Properties section of My Computer)
* Improve the security of your Web browser by preventing it from automatically running the potentially dangerous programs that are sometimes contained within webpages you visit. If you are using Mozilla Firefox, you can install the NoScript add-on.
* Download over an encrypted connection (usually SSL in the browser) whenever possible.
* Using free and open-source software significantly lowers your risk of being infected by malware. These tools are often written and updated for free by volunteers and are generally more secure than their proprietary alternatives. In particular, you should consider replacing Internet Explorer, Outlook and Microsoft Office with Firefox, Thunderbird and LibreOffice, respectively. You should also consider switching from the Microsoft Windows operating system to a more secure open-source alternative like Ubuntu or ChromeOS.

**3. Preventing untrusted network connections**

* A firewall helps to protect your computer from unauthorised connections to and from the Internet. It can also help reduce the spread of malware if you are infected. Most operating systems have firewalls included but check to make sure they are turned on. (You can usually find this under Control Panel > Security) There are also excellent free programs such as [*Comodo Personal Firewall*](https://securityinabox.org/comodofirewall_main), which can help keep your computer secure.
* Make sure that all of the computers on your office network have a firewall installed. Only install essential programs on the computer you use for sensitive work, and make sure you get them from a reputable source. Uninstall any software that you do not use.

**4. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for basic advice on how to identify and protect yourself against malware.**

*FURTHER READING*

* [*EFF - How do I protect myself against malware*](https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware)
* [*Security in a Box - Chapter 1, Malware*](https://securityinabox.org/chapter-1)

***Malware Advanced Checklist***

* ***Running anti-virus***
  + ***Run only one anti-virus at a time***
  + ***Update your anti-virus regularly***
  + ***Enable your anti-virus’s 'always on' virus-detection feature***
  + ***Scan your files regularly***
* ***Preventing infection***
* ***Open attachments via applications***
* ***Check where URLs lead***
* ***Disable ‘AutoPlay’***
* ***Prevent auto-running in your browser***
* ***Download over SSL***
* ***Use open-source software***
* ***Use open-source operating platform***
* ***Preventing untrusted connections***
* ***Turn on your firewall***
* ***Keep only essential programs***

**PASSWORDS**

*BASIC*

**1. Why are passwords important?**

Passwords are often the first and only barrier between your information and anyone who might want to read, use or destroy it without your permission.

In general, when you want to protect something - whether a house or an email account - you lock it up with a key. All keys, physical and electronic, have one thing in common: they open their locks just as effectively in the hands of somebody else. You can use the most advanced security tools, but if your password is weak, or if you allow it to fall into the wrong hands, they will not do you any good.

**2. How to make a strong password**

A password should be difficult for a computer program to guess, difficult for others to figure out, and should be chosen so as to minimise damage if someone does learn it.

* **Make it long:** The longer a password is, the longer takes to guess it. Use more than ten characters or ideally a long phrase or sentence. Short passwords of any kind, even totally random ones, are not strong enough for use with encryption today.
* **Make it complex:** Include upper case letters, lower case letters, numbers and symbols.
* **Don't make it personal:** Don't choose a word or phrase based on information such as your name, telephone number, child's name, pet's name, birth date, or anything else that a person could learn by doing a little research about you.
* **Keep it secret:** Do not share your password with anyone unless it is absolutely necessary. If you must share a password with a family member or colleague, you should change it to a temporary password first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a password, such as creating a separate account for each individual who needs access. Keeping your password secret also means not allowing anyone to see you typing it in.
* **Make it unique:** Avoid using the same password for more than one account. Otherwise, anyone who learns that password will gain access to even more of your sensitive information.
* **Keep it fresh:** Change your password on a regular basis, at least once every three months. The longer you keep one password, the more opportunity others have to figure it out and use it.
* **Make it memorable:** If you have to write your password down because you can't remember it, you may end up facing a whole new category of threats that could leave you vulnerable to anybody with access to your work area. If you are unable to think of a password that is long and complex but still memorable, the remembering secure passwords section, below, might be of some help. If not, you should still choose something secure, but you may need to record it using a secure password database such as *KeePass*, outlined in our Advanced lesson. Other types of password-protected files, including Microsoft Word documents, should not be trusted for this purpose, as many of them can be broken in seconds using tools that are freely available on the internet.

**3. Remembering secure passwords**

There are a few tricks that might help you create passwords that are easy to remember but very difficult to guess.

* Vary capitalisation, such as: 'My naME is Not MR. MarSter'
* Alter numbers and letters, such as: 'a11 w0Rk 4nD N0 p14Y'
* Incorporate symbols, such as: 'c@t(heR1nthery3'
* Use multiple languages, such as: 'Let Them Eat 1e gateaU au ch()colaT'
* Use acronyms: 'Are you happy today?' becomes 'rU:-)2d@y?'

A little effort to make the password more complex goes a very long way. Increasing the length of a password even just by a few characters, or by adding numbers or special characters, makes it much more difficult to crack.

You can check the strength of passwords on [Passfault](https://passfault.appspot.com/password_strength.html).

**4. Security Questions**

Be aware of the “security questions” (such as “What is your mother’s maiden name?” or "What was your first pet's name?") that websites use to confirm your identity if you do forget your password. Honest answers to many security questions are publicly discoverable facts that a can be easily found, and therefore bypass your password entirely. Instead, give fictional answers that, like your password, no one knows but you. For example, if the password question asks you your pet’s name, you may have posted photos to photo sharing sites with captions such as “Here is a photo of my cute cat, Spot!” Instead of using “Spot” as your password recovery answer, you might choose “Rumplestiltskin.”

**5. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on how to manage your passwords.**

**Go to the Expert lesson for advice on what to do if you think you might be forced to hand over your password.**

***Passwords Basic Checklist***

* ***Create a strong password***
  + ***Make it long***
  + ***Make it complex***
  + ***Make sure it’s not personal***
  + ***Keep it secret***
  + ***Make it unique***
  + ***Change it regularly***
  + ***Make it memorable***
  + ***Give fake answers to security questions***
* ***Check the strength of passwords on Passfault***
* ***Change old or weak passwords***
* ***Change weak answers to security questions***

*ADVANCED*

**1. Recording passwords securely**

Our Beginner lesson showed you how to create a strong, memorable password. However, because you need a different password for every account or service and also need to change them every few months, it can soon become difficult to remember them all. Fortunately, there are software tools to help with this – a password manager is a software application that can generate random, secure passwords for each of your accounts and record them in a portable, encrypted password database, such as *KeePass*.

The password manager protects all of your passwords with a single master password so you only have to remember one thing. Of course, if you use this method, it becomes especially important that you create and remember a very secure password for *KeePass*, or whatever tool you choose. Whenever you need to enter a password for a specific account, you can look it up using only your master password, which makes it much easier to follow all of the suggestions above.

*KeePass* sits on your desktop, and it also portable, which means that you can put the database on a USB memory stick in case you need to look up a password while you are away from your primary computer.

You can learn how to set up and use this tool in the Keepass tool guide.

**2. Tips for using password managers**

There are few things to keep in mind when using password databases.

* If you lose or accidentally delete your only copy of a password database, you will no longer have access to any of the accounts for which it contained passwords. This makes it extremely important that you back up your *KeePass* database. Read our Backing Up lesson for instructions on how to do this.
* If you forget your *KeePass* master password, there is no way to recover it or the contents of the database. So, be sure to choose a master password that is both secure and memorable!

It is also crucially important to keep your password manager itself secure.

* Some password managers will offer to store your passwords “in the cloud,” which is to say, they will store your passwords encrypted on a remote server, and when you need them on a laptop or mobile, they will retrieve and decrypt them for you automatically. Password managers like this are more convenient, but the trade-off is that they are more vulnerable to attack. If you just keep your passwords on your computer, then someone who can take over your computer may be able to get hold of them. If you keep them in the cloud, your attacker may target that also. It's not usually a compromise you need to worry about unless your attacker has legal powers over the password manager company or is known for targeting companies or internet traffic.
* When you use a password manager, the security of your passwords and your master password is only as strong as the security of the computer where the password manager is installed and used. If your computer or device is compromised and spyware is installed, the spyware can watch you type your master password and could steal the contents of the password safe. So it's still very important to keep your computer and other devices clean of malicious software when using a password manager. You can learn more about this in the Malware lesson.

**3. Two-step authentication**

Many services and software tools let you use two-step authentication. Here the idea is that in order to log in, you need to be in possession of a certain physical object: usually a mobile phone, but, in some versions, a special device called a security token. Using two-step authentication ensures that even if your password for the service is hacked or stolen, the thief won't be able to log in unless they also have control of a second device, such as your phone, and the special codes that only it can create.

Two-step authentication using a mobile phone can be done in two ways: the service can send you an SMS text message to your phone whenever you try to log in which provides an extra security code that you need to type in. Alternatively, your phone can run an authenticator application, such as Google Authenticator, that generates security codes from inside the phone itself. This will help protect your account in situations where an attacker has your password but does not have physical access to your mobile phone.

**4. One-time passwords**

Some services, such as Google, also allow you to generate a list of one-time passwords, also called single-use passwords. These are meant to be printed or written down on paper and carried with you.

There is no way to do this by yourself if you're using a service that doesn't offer it.

If you or your organization runs your own communications infrastructure, such as your own e-mail servers, there's freely available software that can be used to enable two-step authentication for accessing your systems. Ask your systems administrators to look for software offering an implementation of the open standard “Time-Based One-Time Passwords” or RFC 6238.

**5. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to create a strong password.**

**Go to the Expert lesson for advice on what to do if you think you might be forced to hand over your password.**

*RELATED LESSONS/TOOLS*

* Backing Up lesson
* Malware lesson
* KeePass tool guide

*FURTHER READING*

* [*EFF - Creating strong passwords*](https://ssd.eff.org/en/module/creating-strong-passwords)
* [*Security in a Box - Chapter 3, Passwords*](https://securityinabox.org/chapter-3)

***Passwords Advanced Checklist***

* ***Install KeePass***
* ***Create strong password for KeepPass***
* ***Back-up KeePass database***
* ***Ensure computer has no malware***
* ***Install two-step authentication***

EXPERT

**1. Threats of Physical Harm**

Finally, understand that there is always one way that attackers can obtain your password: They can directly threaten you with physical harm or detention. If you fear this may be a possibility, such as if you are going to be travelling across hostile borders with sensitive information, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password. One possibility is to maintain at least one computer/email/keepass account that contains largely unimportant information, whose password you can reveal quickly.

If you have good reason to believe that someone may threaten you for your passwords, it's good to make sure your devices are configured so that it won't be obvious that the account you are revealing is not the “real” one. Is your real account shown in your computer's login screen, or automatically displayed when you open a browser? If so, you may need to reconfigure things to make your account less obvious.

In such circumstances, you should also treat your password manager as a sensitive file, and hide/protect it as we describe in the Protecting Files lesson.

**2. Challenging password demands**

In some jurisdictions, such as the United States or Belgium, you may be able to legally challenge a demand for your password. In [other jurisdictions](https://en.wikipedia.org/wiki/Key_disclosure_law" \t "_blank), such as the United Kingdom or India, local laws allow the government to demand information is given to them. More information on safety precautions to take while travelling can be read in the Journeys lesson.

Please note that intentional destruction of evidence or obstruction of an investigation can be charged as a separate crime, often with very serious consequences. In some cases, this can be easier for the government to prove and allow for more substantial punishments than the alleged crime originally being investigated.

**3. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to create a strong password.**

**Go to the Advanced lesson for advice on how to manage your passwords.**

*RELATED LESSONS/TOOLS*

* Protecting Files lesson
* Journeys lesson

*FURTHER READING*

* EFF - [Defending Privacy at the U.S. Border guide](https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices" \t "_blank)

***Passwords Expert Checklist***

* ***Create & maintain non-sensitive data account***
* ***Make non-sensitive account the primary account on your computer***
* ***Hide/protect your password manager***
* ***Check your rights about disclosure of information***

**PROTECTING FILES**

*ADVANCED*

**1. How to protect sensitive files**

Many human rights activists have sensitive information that could have serious consequences if seen by the wrong people. The Managing Information lesson can help you determine your threat model. Following the steps laid out in the Office lesson and the Malware lesson will help you to protect your computer physically and digitally. However there may be situations where these precautions fail or you need to show your computer to someone whom you don’t want to see the files. This is why you should also protect the files themselves. You can do this by encrypting them so that only you can read them.

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can only be read by someone who has the right encryption key to unscramble it.

Many activists use TrueCrypt, but serious vulnerabilities have recently been found in it. [VeraCrypt](https://veracrypt.codeplex.com/wikipage?title=Downloads) is a good, free, open-source, alternative that we recommend instead. Much like a safe, VeraCrypt creates an encrypted container on your computer or hard drive, that you can put as many files as you like into.

We will shortly be creating a tool guide for VeraCrypt. For now, users can get a step-by-step guide of how to use and install it [here](https://veracrypt.codeplex.com/wikipage?title=Beginner%27s Tutorial).

**2. Tips on using file encryption safely**

There are a few things you should bear in mind when using VeraCrypt and tools like it. No matter how sturdy your safe is, it won't do you a whole lot of good if you leave the door open. When your VeraCrypt volume or container is 'mounted' (what it calls open to view your files), your data may be vulnerable, so you should keep it closed except when you are actually reading or modifying the files inside it.

There are a few situations when it is especially important that you remember to ‘dismount’ (what it calls close) your encrypted volume:

* Dismount it when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, you need to ensure that you do not leave your sensitive files accessible to physical or remote intruders while you are gone.
* Dismount it before putting your computer to sleep.
* Dismount it before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, it is important that you disconnect all encrypted volumes and shut your computer down completely.
* Dismount it before inserting an untrusted USB memory stick or other external storage device, including those belonging to friends and colleagues.
* If you keep an encrypted volume on an external hard drive or a USB stick, remember that just removing the device may not immediately disconnect the volume. Even if you need to secure your files in a hurry, you have to dismount the volume properly, then disconnect the external drive or memory stick, then remove the device.

**3. A secret safe within a safe**

One of the weaknesses with some encryption tools is their visibility – you may be worried that someone could find the encrypted volume, see that you were trying to conceal information, and use intimidation, blackmail or interrogation to force you into opening it.

However VeraCrypt allows you to create a secret volume, inside your regular encrypted volume, to hide your most sensitive information. It is similar to installing a secret 'false bottom' inside your office safe. If an intruder steals your key, or intimidates you into giving them the safe's combination, they will find some convincing decoy material, but not the information that you truly care about protecting.

You open this secret volume by providing an alternate password that is different from the one you would normally use. Even if a technically sophisticated intruder gains access to the standard volume, he will be unable to prove that a hidden one exists.

**4. Hiding your encryption**

If you are concerned about encryption software being found on your computer regardless of what’s in it, there are a few tricks to help disguise VeraCrypt.

* You can rename your encrypted volume to look like a different type of file. Using the '.iso' file extension, to disguise it as a CD image, is one option that works well for large volumes of around 700 MB. Other extensions would be more realistic for smaller volumes.
* You can also rename the VeraCrypt program itself, assuming you have stored it as you would a regular file, rather than installing it as a program. [The VeraCrypt tutorial](https://veracrypt.codeplex.com/wikipage?title=Beginner%27s Tutorial) explains how to do this.

**5. When encryption is illegal**

Encryption is illegal in some countries, which means that downloading, installing or using software of this sort might be a crime in its own right. Any time that merely being associated with encryption software would be enough to expose you to accusations of criminal activity or espionage (regardless of what is actually inside your encrypted volumes), then you will have to think carefully about whether or not such tools are appropriate for your situation.

If that is the case, you have a few options:

* Store only non-confidential information
* Use a system of code words to protect key elements of your sensitive files
* Store all of your sensitive information in a secure webmail account – you would need a reliable network connection and an advanced understanding of computers and Internet services
* Keep sensitive information off of your computer by storing it on a USB stick or portable hard drive – carrying around sensitive, unencrypted information is usually a very bad idea so you would need to keep the device in a very secure place

**6. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* Managing Information Lesson
* Office Lesson
* Malware Lesson
* TrueCrypt Tool Guide

*FURTHER READING*

* [EFF - Encryption](https://ssd.eff.org/en/module/what-encryption)
* [Security in a Box - Chapter 4, Encryption](https://securityinabox.org/chapter-4)

***Protecting Files Advanced Checklist***

* ***Set up VeraCrypt***
* ***Dismount your VeraCrypt volume when not using files***
* ***Create a secret volume for most sensitive material***
* ***Rename your VeraCrypt volume with a different file extension***
* ***Rename the VeraCrypt program***
* ***If encryption is illegal…***
  + ***Store only non-confidential information***
  + ***Use code words***
  + ***Store sensitive information in a secure webmail account***
  + ***Store sensitive information securely off your computer***

**DELETING**

*BASIC*

**1. How to delete information securely**

Most of us think that a file on our computer is deleted once we put the file in our computer's trash folder and empty the trash; in reality, this does not actually delete files – it just makes them invisible to the user until the space they took up on your computer is overwritten with something else. This means that, with the right tools, your “deleted” files can often be retrieved.

The best way to delete a file forever, then, is to make sure it gets overwritten immediately.

This can be done easily using Eraser (for Windows) or Secure Delete (for Mac OS X), both of which are described below. Users of Linux and other open-source operating systems can use GNU shred, but this requires a more advanced technical proficiency.

Note that securely deleting data from solid state drives (SSDs), USB flash drives, and SD cards is very hard! The instructions below apply *only* to traditional disk drives. If you’re using an SSD or a USB flash drive, you can skip to the section about it below.

**2. Secure deletion on Windows**

On Windows, we suggest using Eraser. Eraser is a free/open source secure deletion tool for Windows, and is much better than the built-in tools. To use Eraser, first [download the installer](http://eraser.heidi.ie/download.php" \t "_blank) from its website; make sure to choose a “stable” build. After the file downloads, double-click on it to launch it and Run the file.

Once Eraser is installed, if you want to securely delete a single file or folder, simply:

* Right-click on the file or folder and choose Eraser > Erase from the right-click menu.

Alternatively, you may want to securely erase all the previously deleted data from your computer.

* Launch Eraser.
* Click the downward-pointing arrow next to “Erase Schedule” and choose “New Task.”
* In the “Task Properties” dialog that pops up, set the “Task Type” to “Run immediately.”
* Then click the “Add Data” button near the bottom of the dialog.
* In the new “Select Data to Erase” dialog that pops up, choose “Unused disk space” and make sure the correct disk drive is selected in the drop down box (most likely the “(C:)” drive).
* Click “OK” to exit both dialogs, and Eraser should start erasing.
* Once it’s done erasing, the task will disappear from the list of tasks in the “Erase Schedule.”

**3. Secure deletion on Mac OS X**

On OS X 10.4 and above, you can securely delete individual files by simply:

* Moving them to the Trash;
* Then selecting Finder > Secure Empty Trash.

Alternatively, you may want to securely erase all the previously deleted data from your computer. Apple's advice on this is to:

* Open Disk Utility (in Applications/Utilities);
* Choose Help > Disk Utility Help;
* Search for help on erasing free disk space.

**4. Limitations**

Unfortunately, there are limitations to secure deletion tools. Even if you follow the advice above and you’ve deleted all copies of a file, certain traces of deleted files, such as its name will probably continue to exist for some time on your computer. Overwriting the entire disk and installing a fresh operating system is the only way to be 100% certain that records of a file have been erased.

You may be wondering, "Could I search the raw data on the disk to see if there are any copies of the data anywhere?" The answer is yes and no. Searching the disk will tell you if the data is present in plaintext, but it won't tell you if some program has compressed or otherwise coded references to it. Also be careful that the search itself does not leave a record!

**5. Secure deletion when discarding hardware**

**Computers and hard-drives**

If you want to finally throw a piece of hardware away or sell it on eBay, you'll want to make sure no one can retrieve your data from it. And even if you're not getting rid of it right away, if you have a computer that has reached the end of its life and is no longer in use, it's also safer to wipe the hard drive before stashing the machine in a corner or a closet. This can be done easily with a tool such as [Darik's Boot and Nuke](http://www.dban.org/) – there are a variety of tutorials on how to use it across the web, (including [here](http://www.ucd.ie/itservices/itsupport/itsecurity/securitytools/howtousedbantoremovethecontentsfromaharddisk/" \t "_blank)).

**CD-ROMS**

When it comes to CD-ROMs, you should do the same thing you do with paper―shred them. There are inexpensive shredders that will chew up CD-ROMs. Never just throw a CD-ROM out in the rubbish unless you're absolutely sure there's nothing sensitive on it.

**Solid-state disks (SSDs), USB flash drives, and SD cards**

Unfortunately due to the way SSDs, USB flash drives, and SD cards work, it is difficult, if not impossible, to securely delete both individual files and free space. As a result your best bet in terms of protection is to use encryption—that way, even if the file is still on the disk, it will at least look like code to anyone who gets ahold of it and can’t force you to decrypt it. You can learn about how to use encryption in the Protecting Files lesson.

**6. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Protecting Files lesson*
* *Darik's Boot and Nuke tool guide*

*FURTHER READING*

* [*EFF - How to delete your data securely*](https://ssd.eff.org/en/module/how-delete-your-data-securely)
* [*Security in a Box - Chapter 6, Secure deleting*](https://securityinabox.org/chapter-6)

***Deleting Basic Checklist***

* ***If Windows user, install Eraser***
* ***Securely delete individual files as needed***
* ***Securely delete all previously deleted data every month***
* ***If getting rid of old hardware, wipe the hard drive***
* ***If throwing out CDs, shred them***
* ***Encrypt SSD, USBs and SD cards***

**BACKING UP**

*ADVANCED*

**1. Why back-up?**

Backing up is the copying and archiving of computer data so it can retrieve it if something happens to the original. Years of work can disappear in an instant as a result of theft, carelessness, confiscation, or breakage, so it is extremely important to have an up-to-date backup and a well-tested means of restoring it.

Creating an effective backup policy can be tricky for a few reasons:

* The need to store original data and backups in different physical locations;
* The importance of keeping backups confidential;
* The challenge of coordinating among different people who share information with one another using their own portable storage devices.

In addition to backup and file-recovery tactics, this lesson addresses two specific tools, Cobian Backup and Recuva.

**2. Identifying and organising your information**  
The first step to formulating a backup policy is to figure out where all your personal and work information is currently located. This may include the following:

* Email may be stored on the provider's mail server, on your own computer, or both.
* Documents, address books, or chat histories on the computers you use, which may be in the office or at home.
* Information may also be stored on USB sticks, portable hard drives, or CDs.
* Contacts and important text messages on your mobile phone.
* Your website may contain important information or collection of work.
* Don't forget your non-digital information, such as paper notebooks, diaries and letters.

Next, you need to work out which of these files are 'master copies,' and which are duplicates. The master copy is generally the most up-to-date version of a file and is the one you will want to back-up.

You should make a table of all the information types you identified above and for each of them note:

* Whether that information is master copy or duplicate;
* The device or devices they are stored on;
* The physical location that the device is usually kept.

This table will help you see which of your information (or master copies) is only in one location and therefore vulnerable.

**3. Your backup strategy**  
To back up all of the data types listed above, you will need a combination of software and processes. Basically, you need to make sure that each data type is stored in at least two separate locations.

* **Electronic documents** - Create a full backup of the documents on your computer using a program like Cobian Backup, which is described in more detail below. Store the backup on something portable so that you can take it home or to some other safe location. External hard drives, CD/DVDs or USB memory sticks are possible choices. Because this category of data often contains the most sensitive information, it is important to protect your electronic document backups using encryption. You can learn how to do this in the Protecting Files lesson and in the TrueCrypt Guide.
* **Program databases** - If you use a calendar application or an electronic address book, for example, you will need to find the folder in which these programs store their data. Once you have determined the location of your program databases, you can back them up in the same way as electronic documents.
* **Email** - Rather than accessing your email only through a web browser, install an email client like Thunderbird and configure it to work with your account. The Thunderbird Guide explains in detail how to do this. Also most webmail services will provide instructions on how to use such programs and, often, how to import your email addresses into them. If you choose to move your old email messages to your computer so they are not stored on the server for security reasons, make sure that you include them in the backup of electronic documents described above.
* **Mobile phone contents** - To back up the phone numbers and text messages on your mobile phone, you can connect it to your computer using the appropriate software, which is generally available from the website of the company that manufactured your phone. You may need to buy a special USB cable to do this.
* **Printed documents** - Where possible, you should scan all of your important papers, then back them up along with your other electronic documents, as discussed above.

**4. Storage devices**  
Before you can back up your data, you must decide what kind of storage device you will use.

* **USB sticks or external hard drives** – These are inexpensive, offer large capacity, and are easy to overwrite numerous times. USB sticks often have a lifetime of approximately ten years, with external hard drives lasting longer.
* **CDs** – CDs store around 700 Megabytes (MB) of data. You will need a CD burner and blank discs. If you want to erase a CD and update the files stored on it, you will need to have a CD-RW burner and rewritable CDs. All major operating systems, including Windows XP, now include built-in software that can write CDs and CD-RWs. These discs may begin to deteriorate after five or ten years.
* **DVDs** - DVDs store up to 4.7 Gigabytes (GB) of data. They work much like CDs but require slightly more expensive DVD or DVD-RW burner, and appropriate discs. As with a CD, the data written on a normal DVD will eventually begin to fade.
* **Remote server** - A well-maintained network backup server may have almost unlimited capacity, but the speed and stability of your own Internet connection will determine whether or not this is a realistic option. Keep in mind that running a backup server in your own office, while faster than copying information over the Internet, violates the requirement that you keep a copy of your important data in two different physical locations. There are free storage services on the Internet, as well, but you should very carefully consider the risks of putting your information online and you should always encrypt your backups before uploading them to servers run by organisations or individuals whom you do not know and trust.

**5. Backup Software**Cobian Backup is a user-friendly tool that can be set to run automatically, at regularly scheduled times, and to include only files that have changed since your last backup. It can also compress backups to make them smaller. You can learn how to install and run it in our Cobian Backup Guide.

When using these backup tools, there are a few things you can do to help your backup system work smoothly:

* Organise the files on your computer. Try to move all of the folders that contain electronic documents you intend to back up into a single location, such as inside the My Documents folder.
* If you use software that stores its data in an application database, you should first determine the location of that database. If it is not in a convenient location, see if the program will allow you to choose a new location for its database. If it does, you can put it in the same folder as your electronic documents.
* Create a regular schedule to perform your backup.
* Try to establish procedures for all of the staff in your office who do not already have a reliable, secure backup policy. Help your colleagues understand the importance of this issue.
* Make sure to test the process of recovering data from your backup. Remember that, in the end, it is the restore procedure, not the backup procedure, which you really care about!

Once you have backed up your information or created a back-up process, you need to figure out a safe place to store it. Remember, this needs to be a different location to the one where the original information is! (i.e. if backing up your office files, the usb stick you use should not be kept in the office)

**6. Accidental file deletion**

When you delete a file in on your computer, it usually disappears from view, but its contents actually remain. Even after you empty the Recycle Bin, information from the files you deleted can usually still be found on the hard drive. See the Deleting lesson to learn more about this. Occasionally, if you accidentally delete an important file or folder, this security vulnerability can work to your advantage. There are several programs that can restore access to recently-deleted files, including a tool called Recuva - File Recovery, which you can learn how to use in our tool guide.

It is important that you do as little as possible with your computer between deleting a file and attempting to restore it. The longer you use your computer before attempting to restore the file, the less likely it is that you will succeed. This also means that you should use the portable version of Recuva instead of installing it after deleting an important file. (Or better – install it before anything happens!)

While it might sound like a lot of work to implement the policies and learn the tools described in this chapter, maintaining your backup strategy, once you have a system in place, is much easier than setting it up for the first time. And, given that backup may be the single most important aspect of data security, you can rest assured that going through this process is well worth the effort.

**7. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Protecting Files Lesson*
* *Deleting Lesson*
* *TrueCrypt Tool Guide*
* *Thunderbird Tool Guide*
* *Cobian Backup Tool Guide*
* *Recuva – File Recovery Tool Guide*

*FURTHER READING*

* [*Security in a Box - Chapter 6, Backing up*](https://securityinabox.org/chapter-6)

***Backing Up Advanced Checklist***

* ***Make a table with info type, device and location***
* ***Identify your vulnerable information***
* ***Figure out what storage device is right for you***
* ***Install Cobian Backup***
* ***Organise your files to back up***
* ***Back up information on regular schedule***
* ***Install Recuva***
* ***If recovering files, do as little as possible before using Recuva***

IGNORE THIS Paper SUBSECTION FOR NOW – WE WILL SPLIT IT LATER

**PAPER DOCUMENTS**

*ADVANCED*

**How to protect your information from physical threats**

No matter how much effort you have put into building a digital barrier around your computer, you could still wake up one morning to find that it, or a copy of the information on it, has been lost, stolen, or damaged by any number of unfortunate accidents or malicious acts. Anything from a power surge to an open window to a spilt cup of coffee might lead to a situation in which all of your data are lost and you are no longer able to use your computer. A careful risk assessment, a consistent effort to maintain a healthy computing environment and a written security policy can help avoid this type of disaster.

Assessing your risks

Many organisations underestimate the importance of keeping their offices and their equipment physically secure. As a result, they often lack a clear policy describing what measures they should take to protect computers and backup storage devices from theft, severe weather conditions, accidents, and other physical threats. The importance of such policies may seem obvious, but formulating them properly can be more complicated than it sounds. Many organisations, for example, have good quality locks on their office doors, and many even have secure windows; but if they do not pay attention to the number of keys that have been created, and who has copies of those keys, their sensitive information remains vulnerable. When assessing the risks and vulnerabilities that you or your organisation face, you must evaluate several different levels at which your data may be threatened.

Consider the communication channels you use and how you use them. Examples might include paper letters, faxes, landline phones, mobile phones, emails and Skype messages.

Consider how you store important information. Computer hard drives, email and web servers, USB memory sticks, external USB hard drives, CDs and DVDs, mobile phones, printed paper and hand-written notes are all likely possibilities.

Consider where these items are located, physically. They could be in the office, at home, in a trash bin out back or, increasingly, 'somewhere on the Internet.' In this last case, it might be quite challenging to to determine the particular piece of information's actual, physical location.

Keep in mind that the same piece of information might be vulnerable on many different levels. Just as you might rely on anti-virus software to protect the contents of a USB memory stick from malware, you must rely on a detailed physical security plan to protect the same information from theft, loss or destruction. While some security practices, such as having a good off-site backup policy, are helpful against both digital and physical threats, others are clearly more specific.

When you decide whether to carry your USB memory stick in your pocket or sealed in a plastic bag at the bottom of your luggage, you are making a decision about physical security, even though the information you are trying to protect is digital. As usual, the correct policy depends greatly on the situation. Are you walking across town or travelling across a border? Will somebody else be carrying your bag? Is it raining? These are the sorts of questions that you should consider when making decisions like this. Protecting your information from physical intruders

Malicious individuals seeking access to your sensitive information represent one important class of physical threat. It would be a mistake to assume that this is the only such threat to the security of your information, but it would be even more shortsighted to ignore it. There are a number of steps you can take to help reduce the risk of physical intrusion. The categories and suggestions below, many of which may apply to your home as well as your office, represent a foundation upon which you should build in accordance with your own particular physical security situation.

Around the office

Get to know your neighbours. Depending on the security climate in your country and in your neighbourhood, one of two things may be possible. Either you can turn them into allies who will help you keep an eye on your office, or you can add them to the list of potential threats that your security plan must address.

Review how you protect all of the doors, windows and other points of entry that lead into your office.

Consider installing a surveillance camera or a motion-sensor alarm.

Try to create a reception area, where visitors can be met before they enter the office, and a meeting room that is separate from your normal work space.

In the office

Protect network cables by running them inside the office.

Lock network devices such as servers, routers, switches, hubs and modems into secure rooms or cabinets. An intruder with physical access to such equipment can install malware capable of stealing data in transit or attacking other computers on your network even after he leaves. In some circumstances it may be beneficial to hide servers, computers or other equipment in attics, over a fake ceiling, or even with a neighbor, and use them through wireless connection.

If you have a wireless network, it is critical that you secure your access point so that intruders cannot join your network or monitor your traffic. If you are using an insecure wireless network, anyone in your neighbourhood with a laptop becomes a potential intruder. This is an unusual definition of 'physical', but it helps to consider that a malicious individual who can monitor your wireless network has the same access as one who can sneak into your office and connect an ethernet cable. The steps required to secure a wireless network will vary, depending on your access point hardware and software, but they are rarely difficult to follow.

**At your work**

You should position your computer screen carefully, both on your desk and when you are away from the office, in order to prevent others from reading what is displayed there. In the office, this means considering the location of windows, open doors and the guest waiting area, if you have one.

Most desktop computer cases have a slot where you can attach a padlock that will prevent anyone without a key from getting inside. If you have cases like this in the office, you should lock them so that intruders cannot tamper with their internal hardware. You might also consider this feature when purchasing new computers.

Use a locking security cable, where possible, to prevent intruders from stealing the computers themselves. This is especially important for laptops and small desktops that could be hidden inside a bag or under a coat.

**Software and settings related to physical security**

Make sure that, when you restart your computer, it asks you for a password before allowing you to run software and access files. If it does not, you can enable this feature in Windows by clicking on the Start menu, selecting the Control Panel, and double-clicking on User Accounts. In the User Accounts screen, select your own account and click Create a Password. Choose a secure password, as discussed in Chapter 3: How to create and maintain good passwords, enter your password, confirm it, click Create Password and click Yes, Make Private.

There are a few settings in your computer's BIOS that are relevant to physical security. First, you should configure your computer so that it will not boot from the USB device, CD-ROM or DVD drives. Second, you should set a password on the BIOS itself, so that an intruder can not simply undo the previous setting. Again, be sure to choose a secure password.

If you rely on a secure password database, as discussed in Chapter 3, to store your Windows or BIOS passwords for a particular computer, make sure that you do not keep your only copy of the database on that computer.

Get in the habit of locking your account whenever you step away from your computer. On Windows, you can do this quickly by holding down the Windows logo key and pressing the L key. This will only work if you have created a password for your account, as described above.

Encrypt sensitive information on computers and storage devices in your office. See Chapter 4: How to protect the sensitive files on your computer for additional details and pointers to the appropriate Hands-on Guides.# Portable devices

Keep your laptop, your mobile phone and other portable devices that contain sensitive information with you at all times, especially if you are travelling or staying at a hotel. Travelling with a laptop security cable is a good idea, although it is sometimes difficult to find an appropriate object to which you can attach one. Remember that meal times are often exploited by thieves, many of whom have learnt to check hotel rooms for laptops during hours of the day when they are likely to be unattended.

If you have a laptop, tablet or other mobile device, try to avoid putting them on display. There is no need to show thieves that you are carrying such valuable hardware or to show individuals who might want access to your data that your shoulder bag contains a hard drive full of…

II

Creating your physical security policy

Once you have assessed the threats and vulnerabilities that you or your organisation face, you must consider what steps can be taken to improve your physical security. You should create a detailed security policy by putting these steps in writing. The resulting document will serve as a general guideline for yourself, your colleagues and any newcomers to your organisation. It should also provide a checklist of what actions should be taken in the event of various different physical security emergencies. Everybody involved should take the time to read, implement and keep up with these security standards. They should also be encouraged to ask questions and propose suggestions on how to improve the document.

Your physical security policy may contain various sections, depending on the circumstances:

An office access policy that addresses the alarm systems, what keys exist and who has them, when guests are allowed in the office, who holds the cleaning contract and other such issues

A policy on which parts of the office should be restricted to authorized visitors

An inventory of your equipment, including serial numbers and physical descriptions

A plan for securely disposing of paper rubbish that contains sensitive information

Emergency procedures related to:

Who should be notified if sensitive information is disclosed or misplaced

Who to contact in the event of a fire, flood, or other natural disaster

How to perform certain key emergency repairs

How to contact the companies or organizations that provide services such as electrical power, water and Internet access

How to recover information from your off-site backup system. You can find more detailed backup advice in Chapter 5: How to recover from information loss.

Your security policy should be reviewed periodically and modified to reflect any policy changes that have been made since its last review. And, of course, don't forget to back up your security policy document along with the rest of your important data. See the Further reading section for more information about creating a security policy.

**Regular Post / Mail**

*RELATED LESSONS/TOOLS*

*FURTHER READING*

***Malware Basic Checklist***

* ***Create…***
  + ***Make it…***