# Module 1 – Digital Skills for Green Entrepreneurs

## Unit 7: Security and problem-solving

Co-funded by the European Union

GREENWORAL: 2021-1-ES01-KA220-ADU-000033740

June 2024

Edited By: Dr. Francisca Rosique Contreras
Polytechnic University of Cartagena
June 2024

**Team of authors:**

**Spain: Polytechnic University of Cartagena –** Dr. Francisca Rosique, Dr. Mª Dolores de Miguel, Dr. Hayet Kerras, Dr. Soledad Martínez, Dr. Juan Jesús Bernal, Dr. Víctor García, Dr. Djamil Kahale, Dr. Eva Tomaseti; **CEA Mar Menor –** Francisco Riquelme, Rosario Ros, Violeta Alcaraz; **Francisco de Vitoria University -** Dr. Susana Bautista

**Ireland: Dublin University of Technology –** Dr. Lucia Walsh, Dr. Niamh Imbusch, Deirdre Treacy, Fiona Whelan; **The Mill Business Center -** Anna Maklakova

**Latvia: Technic University of Riga -** Kārlis Valtiņš, Zane Rutkovska, Anete Veide, Lily Bethencourt, Zanda Raciborska, Simona Ozolina-Ugore; **Leader -** Aiva Vīksna, Vita Zariņa

**Cyprus: Cyprus University of Technology** – Ifigeneia Pappa, Dr. Dimitris Tsaltas; **WARL-** Anna Kosma, Georgia Piitaridou

https://greenworal.com/
Project reference: 2021-1-ES01-KA220-ADU-000033740

The "Greenworal" project is co-funded by the European Union. The opinions and views expressed in this publication are the responsibility of the author(s) and do not necessarily reflect the views of the European Union, the European Education and Culture Executive Agency (EACEA), or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union, EACEA, nor the SEPIE National Agency are responsible for them.

# Index

# Unit 7: Security and problem-solving

The use of new technological supports, networks, devices or cloud computing has become a reality of our day to day, both in the role we play, as citizens, employers or employees. Many companies base their activity on information systems, thus becoming the target of cybercriminals who take advantage of their vulnerabilities to carry out their criminal activity. In addition, there are many other threats, both external and internal, intentional or accidental.

In order to reduce all the threats that can negatively affect our activity on the network, we must apply certain basic security measures related to access control, security in operations, and recovery from loss of information. In this unit, we will see a series of fundamental recommendations or good practices that will contribute to significantly reducing the risks to which, as we have seen, we are exposed on a daily basis.

## 1. Cybersecurity tools

Computer security tools are the order of the day in many organizations, since in an increasingly digitized world it is important to protect our most sensitive information.

Computer security is achieved through training employees so that they know how to treat company data, protocols for acting and reacting to cyberthreats and also, of course, with the use of software and other digital security tools that provided by various providers.

Below we are going to review which are the most interesting computer security tools on the market, what they can contribute to us and why we should use them in the workplace to avoid damage to our files.

*Image 1: Cybersecurity tools.*

## 1.1. Types of computer security tools

Below we are going to review which are the most interesting computer security tools on the market, what they can contribute to us and why we should use them in the workplace to avoid damage to our files.

### 1.1.1. Anti-virus software

It seems basic, but you must remember it just in case. Any device that connects to the network, whether personal or corporate, should necessarily have an antivirus. These programs are essential and are mainly responsible for detecting malware infections or other malicious elements.

In other words, antivirus software is a program designed to prevent, detect, and remove viruses and other malware attacks on the computer, networks, and individual IT systems. It also protects computers and networks from a wide variety of threats and viruses, such as Trojans, worms, adware, ransomware, etc.

On the other hand, most antivirus programs come with an automatic update feature allowing the system to check for new viruses and threats on a regular basis. Also, they usually provide some additional services like scanning emails to make sure they are free of malicious attachments or links.

### 1.1.2. Firewall

Many people may consider them obsolete or unimportant, but the reality is that firewalls are essential cybersecurity tools for blocking threats. And although the oldest ones had very simple structures and were only effective against easy threats, today there are more advanced versions capable of classifying files according to many parameters. Its main function is to inspect web traffic, identify users and block unauthorized access.

It is the core of cybersecurity tools. Its job is to prevent unauthorized access to a private network, and it can be implemented as hardware, software, or a combination of both. All messages entering or leaving the intranet pass through the firewall, and the firewall examines and blocks those that do not meet specific security criteria.

On the other hand, although it is very useful, it also has limitations. A skilled cybercriminal could create data and programs that pass as trusted firewalls to remain undetected. Despite this, they are still very useful in protecting our system from less sophisticated malicious attacks.

### 1.1.3. Pentesting

Pentesting or penetration tests are one of the best ways to evaluate our company's security systems and the security of an IT infrastructure, since it tries to take advantage of vulnerabilities safely. These vulnerabilities exist in operating systems, services, and applications, misconfigurations, or risky end-user behaviour.

In penetration testing, cybersecurity experts will use the same techniques and processes that hackers use to detect potential threats and areas of weakness.

In summary, it consists of attacking different environments or systems to detect and prevent possible failures. It is a technique to find those errors in the system. It is one of the practices most in demand today, since thanks to this type of examination, companies can remedy their weaknesses before cybercriminals do. A pen tester is a computer security auditor. They are divided into two:

- Red team, the most offensive part
- Blue team, the defensive part

They are useful for different reasons. Firstly, because they determine the chance of success of a cyber-attack, which vulnerabilities are the highest and lowest risk for the company, which of them can put the organization at risk and which are almost impossible to detect. They also check the ability and efficiency of computer scientists when responding to possible attacks.

### 1.1.4. Staff training

Finally, while staff training is not a cybersecurity tool itself, having employees with basic cybersecurity knowledge is one of the strongest forms of defence against cyberattacks.

There are many tools and forms of training available that can educate company personnel on cybersecurity best practices. All companies can carry out various training techniques to educate their employees so that they can understand their role in security.

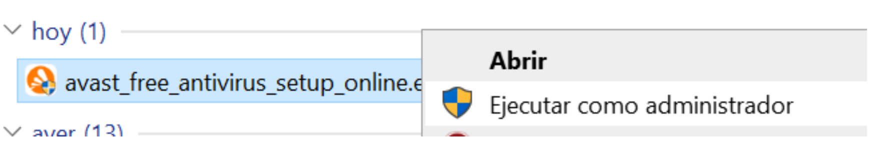
Failure to do so can leave the organization in a position where hackers could easily attack the security system. Therefore, the expense of investing in these training tools could pay off for the business organization with long-term safety and security.

## 1.2. Guided activity: Antivirus installation

In the following activity we are going to see how to install Avast Free Antivirus, one of the most used free antiviruses currently. Avast Free Antivirus for Windows is an essential security application that prevents viruses, spyware, and other malicious applications from infecting your PC. The steps are:

1. Click on the following link https://www.avast.com/en-us/download-thank-you.php?product=FAV-ONLINE&direct=1 to download the Avast Free Antivirus setup file and save it to a known location on your PC (by default, downloaded files are saved in the Downloads folder).

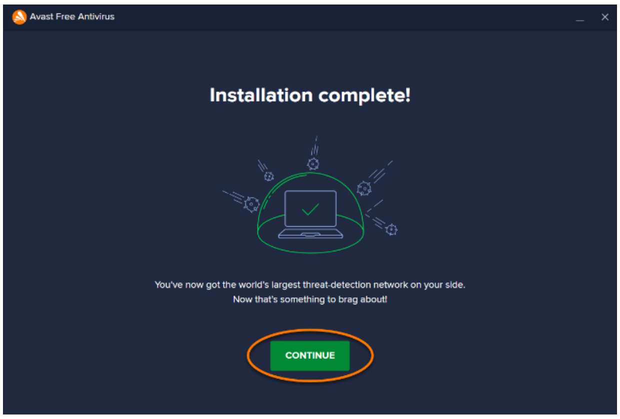
2. Right-click the downloaded avast_free_antivirus_setup_online.exe installation file and select “Run as administrator” from the context menu.



hoy (1)
avast_free_antivirus_setup_online.e
ayer (13)

*Image 2: Option run as administrator from the contextual menu.*

1. If you are prompted for permissions in the User Account Control dialog box, click Yes.
2. To change the default installation language, click the current language in the upper right corner of the screen. Then click Install to proceed with the default installation or click Customize if you need to make changes to the default settings.
3. Wait while the wizard installs Avast Free Antivirus on your PC.
4. When the installation is complete, click Continue.



Installation complete!

You've now got the world's largest threat-detection network on your side.
Now that's something to brag about!

*Image 3: Final screen of the installation.*

5. Click Run First Scan to launch a comprehensive Smart Scan, which detects viruses, malware, problematic browser plug-ins, and other problems on your PC.

With these steps, Avast Free Antivirus should be installed on your PC and ready to use, but some components may not work fully until you restart your PC.

After completing Smart Scan each part of the scan can review the results. When a green check mark appears next to a scanned area, it means that no problems were found in that area. A red exclamation point indicates that one or more problems were found.

The following types of problem can be detected:

- **Viruses - Files** that contain malicious code, which can affect the security and performance of your PC. Check the box next to an unprotected threat, and then click Resolve. It is recommended to select all unprotected threats and click Resolve All. It is not recommended to check Skip at this time when unprotected threats are found.
- **Vulnerable Software - Outdated software** that hackers or hackers can use to gain access to your system. Check the box next to an out-of-date app, and then click Update. You can also click Skip for now to resolve later.

- **Harmful browser plug-ins**: Browser extensions that are usually installed without your knowledge and affect system performance. Check the box next to the plugin, and then click Remove to remove it from the browser. You can also click Skip for now to resolve the vulnerability later.
- **Harmful search engines**: Default search providers that may deliver poor search results or put your privacy at risk. Check the box next to a search engine, and then click Change. Use the dropdown menu to select a new search engine, and then click Change to confirm. You can also click Skip for now to resolve the vulnerability later.
- **Network problems**: vulnerabilities in the network that can lead to attacks on the router and network devices. Check the box next to an unprotected threat, and then click Resolve. You can also click Skip for now to resolve the vulnerability later.
- **Performance problems**: Junk files and unnecessary applications or problems with options that can interfere with the operation of the PC.

### Task 1: Perform a Security Analysis

In this task you should run a smart scan with Avast, save a screenshot of the result, and then try to resolve any detected PC virus threats.
Retest and save a screenshot of the new result.
Send the two screenshots to the Virtual Classroom to verify that the virus threats have been resolved.

## 2. Netiquette

Netiquette (from net and etiquette), Castilianized as Netiquette, or Net Label, is used to refer to the set of rules of general behaviour on the Internet.

Netiquette is nothing more than an adaptation of the etiquette rules of the real world to the virtual one. Although usually etiquette tendencies have evolved to even become part of the rules of certain systems, it is quite common for etiquette rules to be based on an "honour" system; that is to say, that the offender does not even receive a reprimand. In the same way that there is a protocol for physical encounters with people, so-called netiquette describes a protocol to be used when making electronic "contact".

It is important to note that they have been promoted by Internet users themselves to provide greater security and humanity to communication and thus combat network problems such as fraud, spam (junk mail) or rumours. If all users correctly apply the code of ethics on the Internet, cybernetic coexistence will be pleasant, possibly more secure and reliable.

## 2.1. The top ten rules of netiquette

The following list of basic rules, and accompanying explanations, are taken from the book “Netiquette” written by Virginia Shea. They are offered here as a set of guidelines for behaving in cyberspace. They won't answer all your questions, but they will give you some essential principles to help you solve your "Netiquette" dilemmas.

**Rule No. 1:** Remember the human – Good manners.

Normally on the Internet we are anonymous, treat the people with whom you communicate with respect, measure the words you say, because what you write can be archived and then used against you, in general treat others how we would like to be treated.

**Rule No. 2:** Behave like in real life.

Be respectful and behave according to the laws of society and cyberspace, since in cyberspace the chances of being discovered seem remote, but this should not make us forget that there is a human being on the other side of the computer.

**Rule No. 3:** Know where you are in cyberspace.

Before participating in an activity on the Internet, you must observe the conduct, customs and read the rules of the site. Since they do not all work in the same way, and you can make mistakes for not being informed.

**Rule No. 4:** Respect the time and bandwidth of others.

Before sending information to a certain person, make sure that what you send is important, be brief and concise, since the time of others is valuable, and they stop doing other activities to spend time reading what you sent.

**Rule No. 5:** Form of writing.

Use good writing and grammar to write your emails, be clear and coherent with the information you transmit so that it is not distorted; be simple, nice, polite and avoid using offensive language because it may upset someone.

**Rule No. 6**: Share expert knowledge.

Share your knowledge and that of the other experts with other people on the network and make cyberspace a medium to teach and communicate what you know. Put yourself in the place of others and remember when you didn't know a subject, what they ask you about now.

**Rule No. 7:** Help keep disputes under control.

When you want to join a conversation like in a forum, do it when you are sure of what you are going to write. Do not distribute dubious information without verifying whether it is true or not.

**Rule No. 8:** Respect for the privacy of others.

If you share the computer with other members or users, respect their data. Do not read other people's emails, do not look at their files, etc. This is applicable both to users who use your computer and to other users who do not.

**Rule No. 9:** Do not abuse the advantages that you may have.

Not taking advantage of the advantages that you may have due to knowledge or access to different systems that you know about, does not give you the right to take advantage of others.

**Rule No. 10:** Excuse the mistakes of others.

Remember that we are all human and therefore we all make mistakes. You should never judge someone for their failures. In any case, help him or suggest him when an error is found and never show arrogance when finding a mistake, much less laugh at it.

## 3. Electronic certificate

The electronic certificate is a digital signature that is installed in the browser to guarantee your identity on the Internet and that allows you to carry out procedures from your computer, mobile device, or tablet in our Electronic Office and in other organizations that also accept it.

When you access a procedure that requires an electronic certificate, a window will appear on the screen to choose the appropriate certificate and continue with the procedure.

In Europe, the electronic signature is included in European Regulation 910/2014, of July 23, relating to electronic identification and trust services; better known as the eIDAS Regulation, adopted with the idea of regulating the legal framework for the use of electronic signatures in the different Member States of the European Union.

As established by the eIDAS Regulation, there are three levels of electronic signature:

- The simple electronic signature
- The advanced electronic signature
- The qualified electronic signature

Of all of them, the advanced electronic signature is the most used by companies, because it provides much more security than a simple electronic signature and, on the other hand, its use is much simpler, accessible and less expensive than that of the signature qualified electronics.

GREENWORAL

“Training and mentorship based adult rural women empowerment in the field of green entrepreneurship”

Universidad Politécnica de Cartagena

MEMBER OF EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Universidad Francisco de Vitoria UFV Madrid

CEA marmenor

1862 RIGA TECHNICAL UNIVERSITY

LĪDERE

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

the mill
Drogheda's Enterprise Hub

Cyprus University of Technology

Σύλλογος Γυναικών
ΥΠΑΙΘΡΟΥ ΛΑΡΝΑΚΑΣ