DIGITAL ACCESS

DIGITAL SKILLS FOR PEOPLE LIVING IN THE 3RD AGE
Effective Digital Access to Public Services

Erasmus+

DIGITAL ACCESS PROJECT

LEARNING MODULE

Intermediate online safety knowledge

Prepared by: AKLUB

September 2018

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

Obsah

WORKLOAD: [ALL UNITS LEARNING HOURS + OVERALL TIME FOR THE EXERCISES]

SUMMARY

This module designed to expand basic user's knowledge of online safety that are used to exploit the uninitiated or novice user of the internet. The unit's primary objectives is to empower the user to guard against cyber criminals and to keep personal information safe ensuring their online data and assets are not compromised.

KEYWORDS

Home wireless network, Antivirus program, Virus, Malware, antispyware program, spyware

MODULE OBJECTIVES

Actions / Achievements		
Acquiring an understanding of internet based criminal activities targeted at individuals and the acquisition of the skills to identify and avoid these activities.		
Knowledge	**Skills**	**Competencies**
Securing of internet connections	Understanding Home wireless network Know how to set it up Know rules for its safety	Being able to set up and manage security of your Home wireless network
Antivirus programs	Understanding viruses and need of antivirus programs Be able to choose suitable antivirus program Know how to avoid viruses in your computer	Know how to protect your computer against virus infection.

Malware	Understanding malware and need of antimalware programs Be able to choose suitable antimalware program Know how to avoid malware in your computer	Know how to protect your computer against malware.

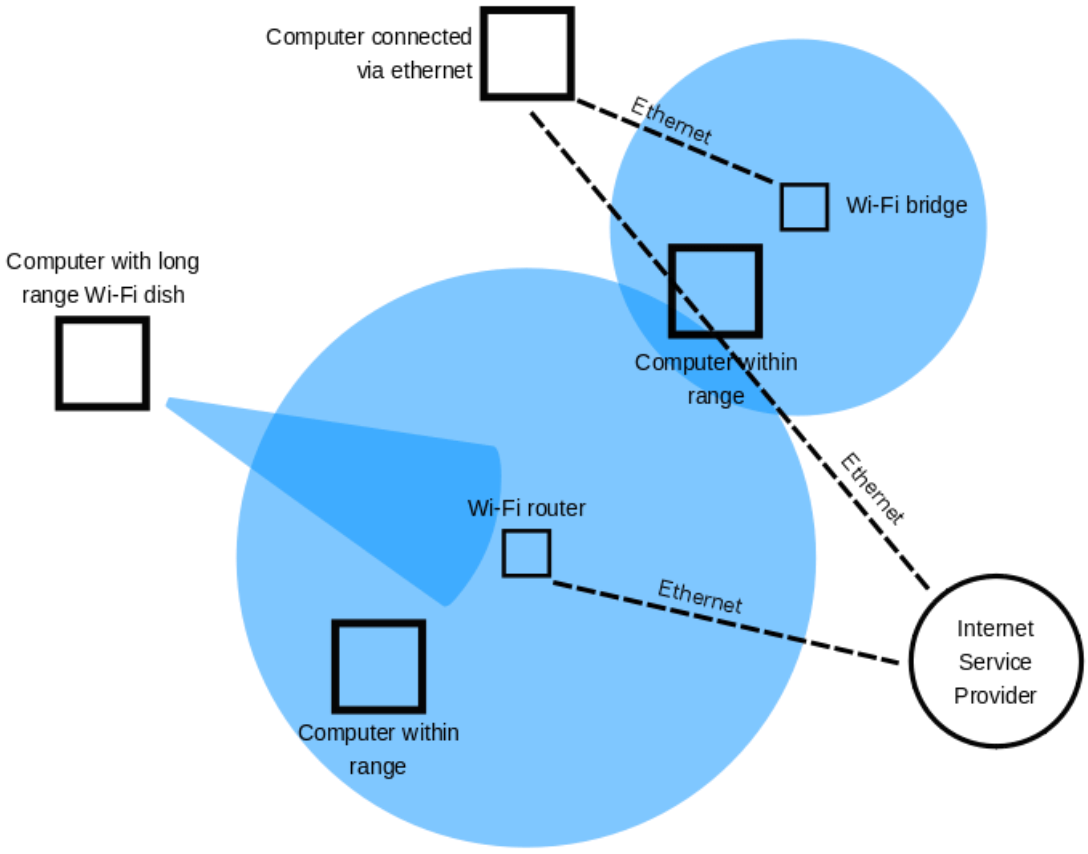
UNIT 1- Securing of Internet connection

Home wireless network

In a few simple words, a basic home wireless network means connecting an Internet access point, such as a cable from your Internet Service Provider, to a (wireless) router in order to allow multiple devices to connect to the network very quickly.

In many cases, once a Wireless router has been installed, we find a place in our home for it and forget about it. As long as all our devices are set up and connected via the Wi-fi network, that's all that matters, right? Wrong!

.



Probably many of you don't realize, but the Internet router is one of the most important devices in our home. It's the gateway to our Internet access and also prone to exploits by cybercriminals who can sneak into our devices and get access to our system.

The only measure most people use to protect their home network is to set up a password and prevent neighbours and other people from taking control over your data. But we have to be more

serious about security and do more than just setting a simple password. A serious risk is that an online criminal might exploit your poor Wi-fi security measures and "listen" to your traffic in order to retrieve sensitive information or take advantage of your network to launch malicious attacks such as Man-in-the-Middle attacks, network sniffing or data theft.

Though relatively easy to use and access, Wi-Fi networks are not always SECURE networks**.** Wi-fi comes with lots of security issues, and it's worth reminding about the Krack vulnerability found in the Wireless Protected Access II (WPA2) protocol which affected all devices connected via Wi-fi.

For this reason, learning how to secure your wireless home network against cybercriminals is a wise and smart move. Given how many Internet of Things devices you may own, making sure your network is extra safe carries even more weight, even though sometimes taking care of your cybersecurity can be a tedious but necessary task.

In this lesson, you will learn how you can better secure your home network and decrease chances of getting your valuable data compromised.

Step 1. Change the name of your default home network

If you want to better secure your home network, the first thing you should do is to change the name of your Wi-Fi network, also known as the SSID (Service Set Identifier).

While giving your Wi-Fi a somewhat provocative name such as "Can't hack this" may backfire at times, other names such as "this is not a wifi" or "too fly for a wifi" are perfectly acceptable.

Changing your Wi-Fi's default name makes it harder for malicious attackers to know what type of router you have. If a cybercriminal knows the manufacturer name of your router, they will know what vulnerabilities that model has and then try to exploit them.

We strongly advise not to call your home network something like "John's Wi-Fi". You don't want them to know at first glance which wireless network is yours when there are probably three or four other neighboring Wi-Fis.

Also, remember that disclosing too much personal information on a wireless network name may expose you to an identity theft operation.

Here's a step-by-step and simple guide that explains how you can easily change the name of your wireless network.

Step 2. Make sure you set a strong and unique password to secure your wireless network

You probably know that every wireless router comes pre-set with a default username and password**,** which is needed in the first place to install and connect your router. The worst part: it's easy for hackers to guess it, especially if they know the manufacturer.

So, make sure you change them both immediately.

A good wireless password should be at least 20 characters long and include numbers, letters, and various symbols**.**

Use this guide to set up a strong password for your network. Friends coming over for a visit may complain about the unusual length of your password, but this might discourage them from needlessly consuming your data with boring Facebook or Instagram posts.

Step 3. Increase your Wi-Fi security by activating network encryption

Wireless networks come with multiple encryption languages, such as WEP, WPA or WPA2.

To better understand this terminology, WPA2 stands for Wi-Fi Protected Access 2 and is both a security protocol and a current standard in the industry (WPA2 networks are almost everywhere) and encrypts traffic on Wi-Fi networks. It also replaces the older and less secure WEP (Wired Equivalent Privacy), and is an upgrade of the original WPA (Wi-Fi Protected Access) technology. Since 2006, all Wi-Fi certified products should use WPA2 security.

WPA2 AES is also a standard security system now, so all wireless networks are compatible with it. If you want to enable WPA2 encryption on your Wireless router, use these six steps. If you are using a TP-Link wireless router, here's how to secure your wireless network.

The good news is that the WPA3 is already here and will replace WPA2. The Wi-Fi Alliance recently announced its next-generation wireless network security standard which aims to solve a common security issue: open Wi-Fi networks. More than that, it comes with security enhancements and includes a suite of features to simplify Wi-Fi security configuration for users and service providers.

Step 4. Turn off the wireless home network when you're not at home

In order to secure your network, we strongly recommend you **t**o disable the wireless home network**,** in case of extended periods of non-use. You should do the same thing with all your devices that are using Ethernet cables or when you won't be at home.

By doing this, you are closing any windows of opportunity malicious hackers might attempt to get access to it while you are away.

Here are a few advantages of disabling your wireless network:

- **Security reasons** – Turning off your network devices, it minimizes the chances of becoming a target for hackers.
- **Surge protection** – When you power off your network device, you also lower the possibility of being damaged by electric power surges;
- **Noise reduction** – Although the modern home networks are much quieter these days, disabling your wireless home network can add calmness to your home.

Step 5. Where is the router located in your home?

You probably haven't thought about this in the first, but where your Wi-Fi place in your home is can also have an impact on your security.

Place the wireless router as close as possible to the middle of your house**.** Why? First of all, it will provide equal access to the Internet to all the rooms in your home. Secondly, you don't want to have your wireless signal range reach too much outside your home, where it can be easily intercepted by malicious persons.

For this reason, we recommend not to place your wireless router close to a window since there's nothing to block the signal going outside your home.

Step 6. Use a strong network administrator password to increase Wi-Fi security

To set up your wireless router, you usually need to access an online platform or site, where you can make several changes to your network settings.

Most Wi-Fi routers come with default credentials such as "admin" and "password" which are such an easy for malicious hackers to break into.

Did you know that the number of wireless networks has increased dramatically over the last 8 years? In 2010 there were 20 million Wi-Fi networks around the globe, and in 8 years, that number increased to 400 million.

Step 7. Change your default IP address on the Wireless router

Changing the default IP address to a less common one is another thing you should consider doing to better secure your home network and make it more difficult for hackers to track it.

To change the IP address of a router, you should follow these steps:

1. Log into your router's console as an administrator. These basic steps will teach you how to easily connect to your home network as an admin. Usually, the address bar type looks like http://192.168.1.1 or http://192.168.0.1
2. Once you are there, insert the username and password on the login page;
3. Then select Network > LAN which is in the menu of the left side;
4. Change the IP address to preference, then click Save.

Note: After you've changed the IP address, you'll need to type the new IP address into the web browser bar.

You can also change the DNS server that your Wireless router is using to filter the Internet traffic and this lesson will show how to do it.

Step 8. Turn off the DHCP functionality on the router

To enhance the wireless network security, you should turn off the Dynamic Host Configuration Protocol (DHCP) server in your router which is what IP addresses are assigned to each device on a network. Instead, you should make use of a static address and enter your network settings.

This means that you should enter into your device and assign it an IP address that is suitable to your router.

Step 9. Disable Remote Access

Most routers allow you to access their interface only from a connected device. However, some of them allow access even from remote systems.

Once you turned off the remote access, malicious actors won't be able to access your router's privacy settings from a device not connected to your wireless network.

To make this change, access the web interface and search for "Remote access**" or "**Remote Administration**".**

Step 10. Always keep your router's software up-to-date

The software is an essential part of your wireless network security. The wireless router's firmware, like any other software, contains flaws which can become major vulnerabilities and be ruthlessly exploited by hackers, as this unfortunate family would find out.

Unfortunately, many wireless routers don't come with the option to auto-update their software, so you have to go through the hassle of doing this manually.

And even for those Wi-Fi networks that can auto-update, it still requires you to switch on this setting. But, we remind you about the importance of software patching and how neglecting to do this can leave open doors for cybercriminals to exploit various vulnerabilities. Read what security experts have to say about updating your software and why it is a key to online security.

Step 11. A firewall can help secure your Wi-Fi network

Firewalls aren't just software programs used on your PC, they also come in the hardware variety.

A hardware firewall does pretty much the same thing as a software one, but its biggest advantage is that it adds one extra layer of security.

The best part about hardware firewalls is that most of the best wireless routers have a built-in firewall that should protect your network from potential cyber-attacks. This lesson can help you figure out if your router has a firewall built in and how you can activate it. And we strongly suggest to turn it on t if it's not by default as an extra layer of protection.

If your router doesn't have one, you can install a good firewall device to your router in order to protect your system from malicious hacking attempts against your home network.

Step 12. Enhance protection for the devices most frequently connected to your home network

Important: Do not leave any exposed vulnerabilities for online criminals to pick on!

Even though you've increased protection for your router and home network, you need to make sure you don't have any security holes that can be exploited by online criminals**.**

Here's what we recommend you to do:

1. Remember to always keep your devices up to date with the most recent software available**;**
2. Always apply the latest security patches to ensure no security hole is left open to malicious actors.
3. Check which devices connect most often to your home network and make sure they have antivirus and/or an anti-malware security software installed. If you don't know which one you should choose, this guide will be very useful.
4. Make sure to protect your devices using multiple security layers consisting of specialized security software such as updated antivirus programs and traffic filtering software. You may consider using an antimalware software program.

Conclusion

Securing the home network should be a top priority for each of us interested in keeping the data safe and secure. These steps can be really useful even for the non-tech savvy person to apply.

Also, do not forget that your wireless network security can be sometimes weak, and prone to exploits. It almost doesn't matter how strong your password is or if your software is up to date if cybercriminals can just hijack your Wi-Fi data.

UNIT 2: Antivirus programs

Outcome

Most systems need antivirus software. Here's what to choose, how to install it, and how to use it to keep yourself safe¨

Viruses

It's something we all hope to avoid but the truth of the matter is that we can't dodge it forever. Some of us are the unfortunate acquirers of computer viruses. Following rules helps you to handle to minimalize the risks.

Install an anti-virus program

Whether you are connecting to the internet or not, having reliable protection is the route to go. Anti-virus programs are a minimal investment and are worth the money so as soon as you power up that computer, make sure you are protected! In this lesson you can find link to the reviews for antivirus software. You can choose from free and paid offers, choose the most suitable for you and easily install it from original website.

Avoid suspicious websites

A lot of times websites will notify you if you are about to enter a website that attempts to install or run a program on your computer but not always. Avoid websites such as those.

Never open email attachments without screening them

The most common way viruses are spread remains to be through email. Make sure you use an email provider that requires all attachments to be scanned prior to opening, to ensure your computer doesn't get a virus.

Set up automatic scans

Setting up scans to run on your computer daily or weekly is a good idea to get rid of any viruses. This keeps your computer updated and clear of issues.

Watch your downloads

We understand that downloading files from the internet such as music and movies is what so many of us do, but it also gets so many of us in trouble. Big files like those are easy to sneak some trouble into so be aware of what you are downloading.

Update, Update, Update!

Microsoft Windows 'Critical Update' is one example of staying ahead of all the hackers out there. Critical Update is an entire branch of Microsoft that is dedicated to keeping computers free is viruses. Always keep your system updated

Always be in the know

Whether you are a computer fanatic or you just use yours casually, always know what the latest viruses are and how they will affect your computer. This will prepare you if something happens so you can fix the problem sooner.

Avoid cracked software

Everyone knows that you can download illegal or 'cracked' software online that seems to be easier on the wallet but in reality downloading those programs hurt you. They subject your computer to hard-to-detect bugs and will end up causing you more problems.

Install a firewall

A firewall is a program that screens incoming internet and network traffic. Along with your virus program, it can help prevent unauthorized access to your computer.

Be prepared

If you get wind of a virus that is going around like wildfire than be sure to be on high alert. Don't accept any downloads and be extra cautious when opening emails and files.

This unit should help you in preparing for any computer viruses that could come your way. Remember to always be cautious and smart when using your computer!

UNIT 3: Malware

Outcome

Identifying and dealing with cyberstalking and the avenues to report it.

Malware

Malware, short for "malicious software," refers to a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways. Malware can infect computers and devices in several ways and comes in a number of forms, just a few of which include viruses, worms, Trojans, spyware and more. It's vital that all users know how to recognize and protect themselves from malware in all of its forms.

So what is malware? It comes in a bewildering variety of forms. Computer viruses are probably the most familiar type of malware — so named because they spread by making copies of themselves. Worms have a similar property. Other types of malware, such as spyware, are named for what they do: In the case of spyware, it transmits personal information, such as credit card numbers.

Protecting your computer and personal devices from malware requires both ongoing personal vigilance and help from professional security companies. Nowadays, malware doesn't just target your home computers but also the mobile devices that you and your family are using. And the problem is bigger than you might think.

You can be a victim of a malware attack through your web browsers, email, the social networks you use, instant messaging, and downloaded files.

Your device can be infected through almost any online process or even a friend's USB stick, so it's important to use a security program that can provide complete proactive protection, helping you before you get infected.

So after asking "What is malware?" the next logical questions are, "who is creating it, and why?" The days when most malware was created by teenage pranksters are long gone. Malware today is largely designed by and for professional criminals.

These criminals may employ a variety of sophisticated tactics. In some cases, as technology site Public CIO notes, cybercriminals have even "locked up" computer data — making the information inaccessible — then demanded ransom from the users to get that data back.

But the main risk that cybercriminals pose to heavy computer users is stealing online banking information such as banking and credit card accounts and passwords. The criminal hackers who steal this information may then use it to drain your account or run up fraudulent credit card bills

in your name. Or they may sell your account information on the black market, where this confidential information fetches a good price.

Protecting Against Malware

So now we're at the biggest question of all: "How do I make sure my computer or network is malware-free?"

The answer has two parts: Personal vigilance, and protective tools. One of the most popular ways to spread malware is by email, which may be disguised to look as if it is from a familiar company such as a bank, or a personal email from a friend.

Be wary of emails that ask you to provide passwords. Or emails that seem to be from friends, but have only a message such as "check out this cool website!" followed by a link. Personal vigilance is the first layer of protection against malware, but simply being careful is not enough. Because business security is not perfect, even downloads from legitimate sites can sometimes have malware attached. Which means that even the most prudent user is at risk, unless you take additional measures.

Install Anti-Spyware Software:

Spyware is a software program that collects personal information or information about an organization without their approval. This information is redirected to a third party website. Spyware are designed in such a way that they are not easy to be removed. Anti-Spyware software is solely dedicated to combat spyware. Similar to antivirus software, anti-spyware software offers real time protection. It scans all the incoming information and helps in blocking the threat once detected.

Recommended anti spyware software you can find at the end of the lesson. You can go through and choose the most suitable for you.

No protection is absolute. But a combination of personal awareness and well-designed protective tools will make your computer as safe as it can be.

EXERCISES

Exercise 1: Take control of your Router through unique password:

Step 1: Login to your wireless router.

Open Internet Explorer and type in the address http://192.168.0.1 or http://192.168.1.1 (By default, most router will have **192.168**.0.1
or **192.168.1.1** as the default Router IP address. This is the
address you would enter into your browser's address bar to access the router configuration page.)

Now login to your router. What??. You don't have user ID and password??. Don't worry. I do have you credentials (provided you have not changed it earlier)

Your user ID and password should be:

Five
Characters. All small. 1st alphabet then 4th alphabet then 13th alphabet then 12th alphabet then 14th alphabet

Making it simple for you:

User ID:admin

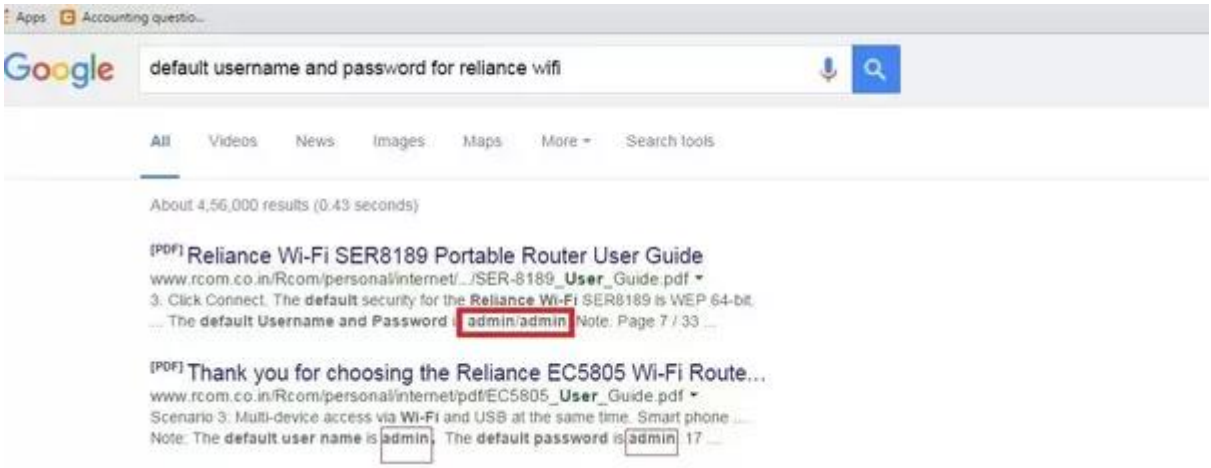
Password:admin

OR

User ID:admin

Password(blank):

If it's not working for you, please google for default user ID/password for your router/service provider.

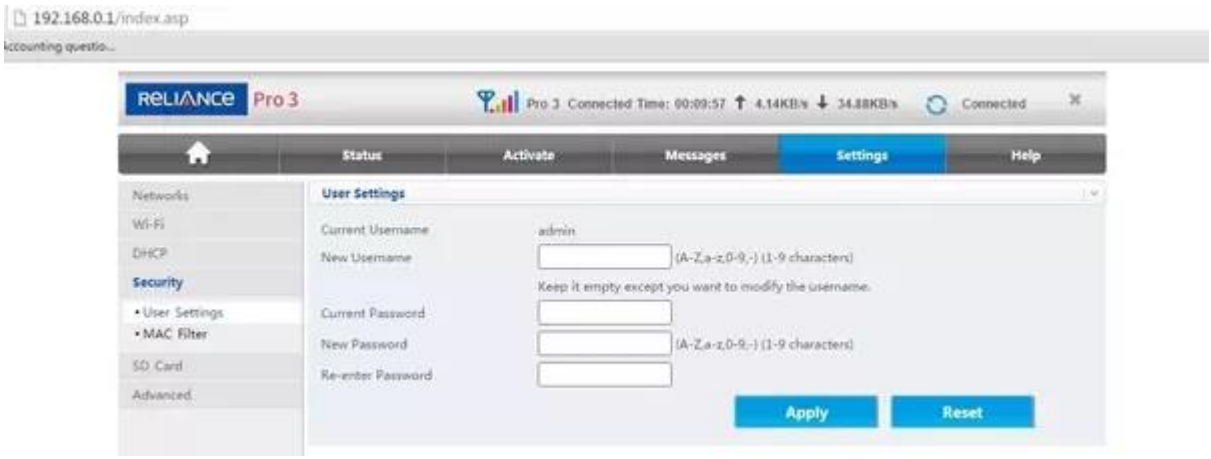


Step 2: Change your USER ID and Password immediately.

-Go to settings

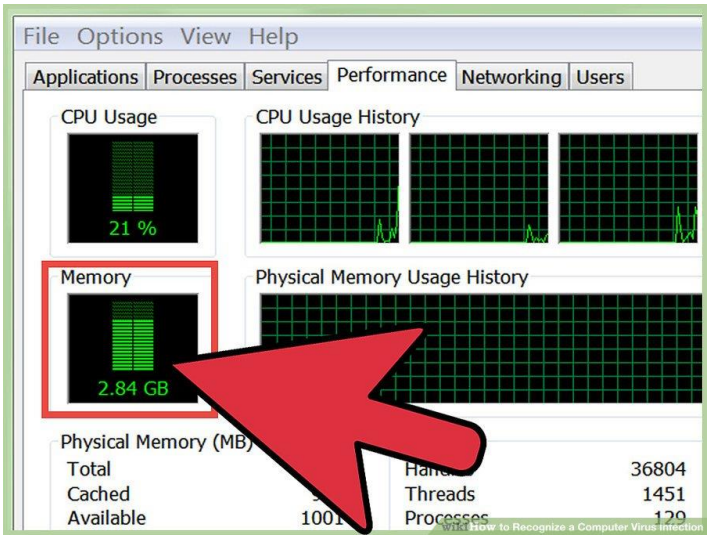
-User Settings

-Update your New Credentials



Exercise 2: Recognize virus on your computer

1. Check your hard drive activity. If you aren't running any programs and your hard drive light is constantly turning on and off, or you can hear the hard drive working, you may have a virus that is working in the background



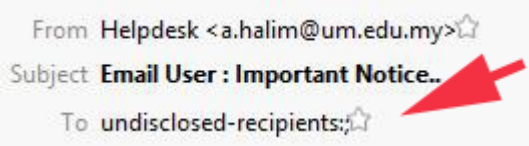
2. Time how long it takes your computer to boot up. If you start noticing that your computer takes significantly more time than usual to start, a virus may be slowing down the startup process.

If you can't log in to Windows, even with the correct log in information, a virus has most likely taken over the log in process.

3 Look at your modem lights. If you don't have any programs running and your modem transfer lights are constantly blinking, you may have a virus that is transmitting data over the network.

Exercise 3: Recognizing a Malware Email

1. **Sender's email address**. If the sender's address is unfamiliar or doesn't match an expected address for a company, then it is probably a malware email. Most malware emails appear to be package delivery notices, invoices, fax/scans, or court notices. These emails rarely appear to come from an appropriate address, for example emails claiming to be from DHL or UPS are likely to be malware if they're From address does not match ups.com or dhl.com.
2. **Email subject or attachment contains username.** A malware email may contain your username in the subject or the attachment filename, or the Subject field may be blank. Contrast this to normal emails which almost always have a Subject and rarely mention your email username.
3. **Enticement to open an attachment.** Many emails containing malware will encourage you to open an attachment. Many attachments can still be harmful even if you are running antivirus. Emails about package delivery problems have no good reason to require you to open an attachment; if they were emailing you about a legitimate delivery problem they could just inform you in the body of the email.
4. **Enticement to follow a link.** Some malware emails are similar to phishing emails where they encourage you to follow a web link. This web link could lead to malware, so please consider all the tips first.
5. **Information verification.** If an email is asking for you to confirm, check, review or provide information using an attachment, it may be a malware attachment. Reconsider if this seems safe and contact support if in doubt. It may not be safe to open the attachment.
6. **Problem warning, threat, or urgency**. Malware emails often attempt to incite your fear, worry, or a sense of urgency. If an email encourages you to solve a problem by opening an attachment then you should be very wary. Some emails appear to be a second response asking you for a follow-up. Examples include dealing with package delivery problems, information about fake court appearances, or fake invoices from entities you may not be doing business with.
7. **Undisclosed-recipients/unlisted-recipients.** If the email recipient list shows undisclosed-recipients/unlisted-recipients or an email address other than yours, then it may be malware.



8. **Suspicious attachment.** If the email has an unexpected attachment such as a file with the extensions .doc, .zip, .xls, .js, .pdf, .ace, .arj, .wsh, .scr, .exe, .com, .bat, or other Microsoft Office file types then it may be malware. Consider that sometimes the file extension is hidden or the contents are different than indicated.
9. **Plain text/absence of logos.** Most legitimate email messages tend to be written with HTML and they may have a mix of text and images. Malware emails rarely have images and tend to have plain formatting.
10. **Generic greeting**. If the email is addressed with a generic phrase like "*Dear Customer*" then it may be malware or a phishing attempt.

11. **Unexpected attachment contents.** If you do ultimately open an attachment and the contents are empty or are very different from what you expected, it may be malware. Please contact support for help immediately! Support may be able to limit damage or help you recover.

What do real malware emails look like?

Here is a real screenshot of a mailbox containing 19 malware emails:

Subject	Correspondents	Date
URGENT RFQ	AL WALEED EQUIPMENTS	03/13/2017 06:55
	starsescorts@gmail.com	03/15/2017 01:27
New Order Attached **KINDLY SEND INVOICE	Amr Hassan	03/15/2017 19:30
We're sad to let you know that our delivery was unusuccessful....	FedEx Expedited Express	03/16/2017 02:53
47929 username2	pkeith@gejlaw.com	03/16/2017 05:29
Delivery Status Notification	webmaster@stroy-exp...	03/16/2017 05:47
	vowsbyjudy@shaw.ca	03/16/2017 14:38
Formal Inquiry	"Anaïs VANACKER"<Va...	03/16/2017 21:16
We have delivery problems with your parcel #7104543	webmaster@whfarm2....	03/17/2017 00:57
INQUIRY	Saigon Offshore	03/17/2017 03:47
	dava@ac-lyon.fr	03/17/2017 14:25
54343 username	juanro5554@hotmail.c...	03/17/2017 14:48
Item Delivery Notification	alifeof8@server.alifeofj...	00:34
UPS courier can not deliver parcel #004287245 to you	webmaster@stroy-exp...	06:23
Parcel Delivery Notification	abidjanbateau@vps286...	06:52
Visa Card Award	info@visa.com	07:21
Problems with item delivery, n.4930349	Apache	09:54
Package Delivery Notification	Apache	10:06
Delivery Status Notification	contrav8@box980.blue...	17:05

Exercise 4: Online safety quiz

Take this quiz online and see how you score.

https://www.proprofs.com/quiz-school/story.php?title=esafety-quiz

FURTHER READING AND RESOURCES

Terms that you should know

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Internet Safety planning for seniors (PDF download)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReqQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Top internet safety tips (PDF download)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC&url=https%3A%2F%2Fquery.prod.cms.rt.microsoft.com%2Fcms%2Fapi%2Fam%2Fbinary%2FRE1ImTu&usg=AOvVaw0QyXRMv5RLg-kAS0tIaUvz

How to protect from malware – Youtube video

https://www.youtube.com/watch?v=uJRqZTNMC

Mo

The best antivirus services for 2018

https://www.itproportal.com/guides/best-antivirus-services-for-2018/

The best antimalware software for 2018

https://www.techradar.com/news/best-free-anti-malware-software

Protecting your data

https://youtu.be/BL7WJM342Uc

Online safety for seniors

https://www.connectsafely.org/seniors/

More online safety info

https://www.protectseniorsonline.com/resources/

How to check if the computer has a virus

https://www.youtube.com/watch?v=4i_cCPhewu4