

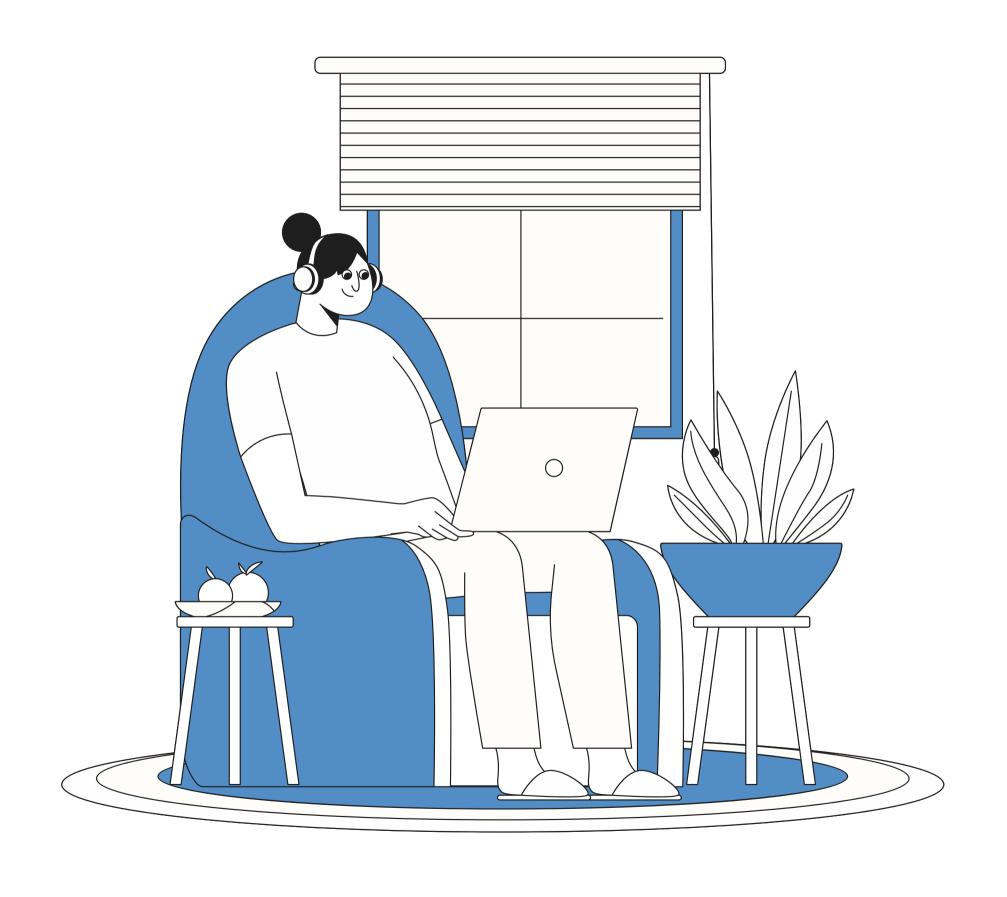


How can Older Persons
protect themselves
from cybercriminals
while making the most
of digital technologies?



### **UNITED NATIONS INTERNATIONAL DAY OF OLDER PERSONS 2021:**

Digital Equity for all Ages: Connect, Respect and Protect Older People in Digital Technologies



# Main types of threat you can face online

### 01

#### Investment scams

Luring you to high return investments

### 03

### Blackmail

Using personal data (photos, videos, private conversation...) to blackmail you for money

### 05

### **Identity Theft**

Using your identity to commit crimes, contract loans or to open fraudulent bank accounts

### 02

### Solidarity fraud

Luring you into false solidarity campaigns

### 04

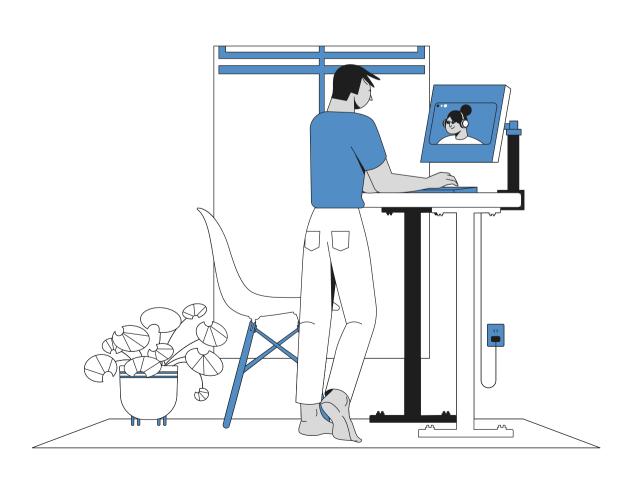
### Money Embezzlement

Cybercriminals taking control of your bank account or credit card

### 06

### Use of your device or accounts to reach a third person

# How does it happen?



Phishing and other computer intrusion "Cyber-based crime"

Social engineering fraud "Cyber-enabled crime"

Frequently a combination of both

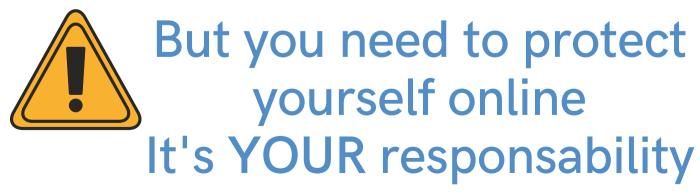
# Should you stay away from social medias and technology?

### You can't

You need internet in your daily life for a lot of administrative and welfare procedure

### You shouldn't

Technology is a chance to remain connected to your family and friend and can brings a lot of opportunities for a healthy and satisfying retirement





How to protect yourself online?

### General advices

- Be careful with people you met online people can easily pretend to be someone else
- Do not share personal information on you or your family on social medias and forums
- Switch your social medias profiles to private profile
- Do not share intimate photos: they can be use to blackmail you
- Disconnect your webcam when you are not using it

## Enhance your IT security

- Use strong passwords and change them regularly
- Use a two factor solution / double key
- Make sure to update regularly your browser on your computer and your smartphone
- Use an anti-virus on your devices

## Avoid email phishing

- Do not open suspicious emails
- Do not click on a link contained in a suspicious email and don't open the enclosed attached files
- Always check the email address of the sender
- In case of doubt : check with the company or person directly on the phone
- Never click on a link enclosed in an email asking you to change your password

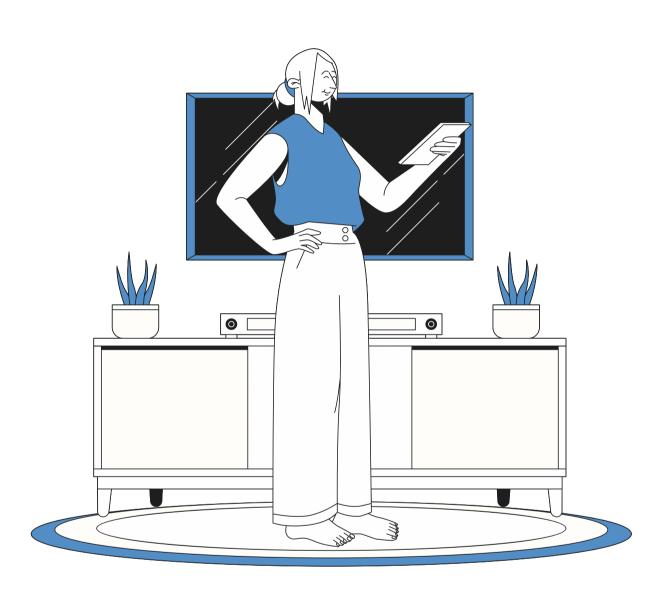
### Avoid Investment scam

- Always trust your bank or financial institution when you are advised to NOT transfer funds to a company or a bank account
- It is not because you started to receive money back from your "investment" that it's not a scam: be aware of ponzi schemes
- Always check if the investment company is regulated (official lists are available on the website of your National Financial Authority)
- Never invest in something you don't understand (forex, wine, cryptocurrencies, livestock...)
- Never invest all your savings in ONE investment product

### Avoid Investment scam

### **RED FLAGS!**

- An Investment company authorized to sell financial products in your country will NEVER ask you to transfer funds to a foreign bank account
- If you are pressured to transfer money to the investment company (insistent phone calls, emails etc.) it is probably a scam. Ask the advice of your financial institution.
- If it is too good to be true: it is probably a scam!



# How to react if you are victim of cybercrime?

- Act quickly: don't wait, don't isolate
- Don't be ashamed, YOU are the victim
- Always report to the police. Bring copies of emails or messages you exchanged with the presumed perpetrators
- Change your password if you still have access to your accounts and report to your financial insititution





# Thank you for your attention



### **UNITED NATIONS INTERNATIONAL DAY OF OLDER PERSONS 2021:**

Digital Equity for all Ages: Connect, Respect and Protect Older People in Digital Technologies