SENIOR SECTECH

ANICA VLAISAVLJEVIC
MADELEINE JANSEN
VERONICA FELICIO
GAYE MIN AYGÜN

Scan me! ☺

INTRO: VULNERABLE ACCESS POINTS

01.

Multiple state studies have shown a massive rise on scams on elderly people.

Research has found increased vulnerability due to a combination of physical, economic, and social factors.

02.

With regards to physical elements, a reduction in cognitive capacities due to deterioration of the prefrontal cortex has been linked to excessive credulousness and diminished financial decision making, thereby increasing vulnerability to fraud.

03.

It is commonly accepted that older generations are less technologically adept than their younger counterparts, and their lack of technological knowledge has been associated with increased risk of cyber fraud victimization. In terms of social factors, social isolation may make older persons easier to manipulate and may reduce their awareness of potential fraud risks.

Negative Trends

- overwhelming information
- exclusive digitalisation
- very fast development

Positive trends

- knowledge is easier to access
- global conections

Headaches

- rush to keep up
- scams

Opportunities

- connections to family and friends
- safe payment
- freetime & hobies

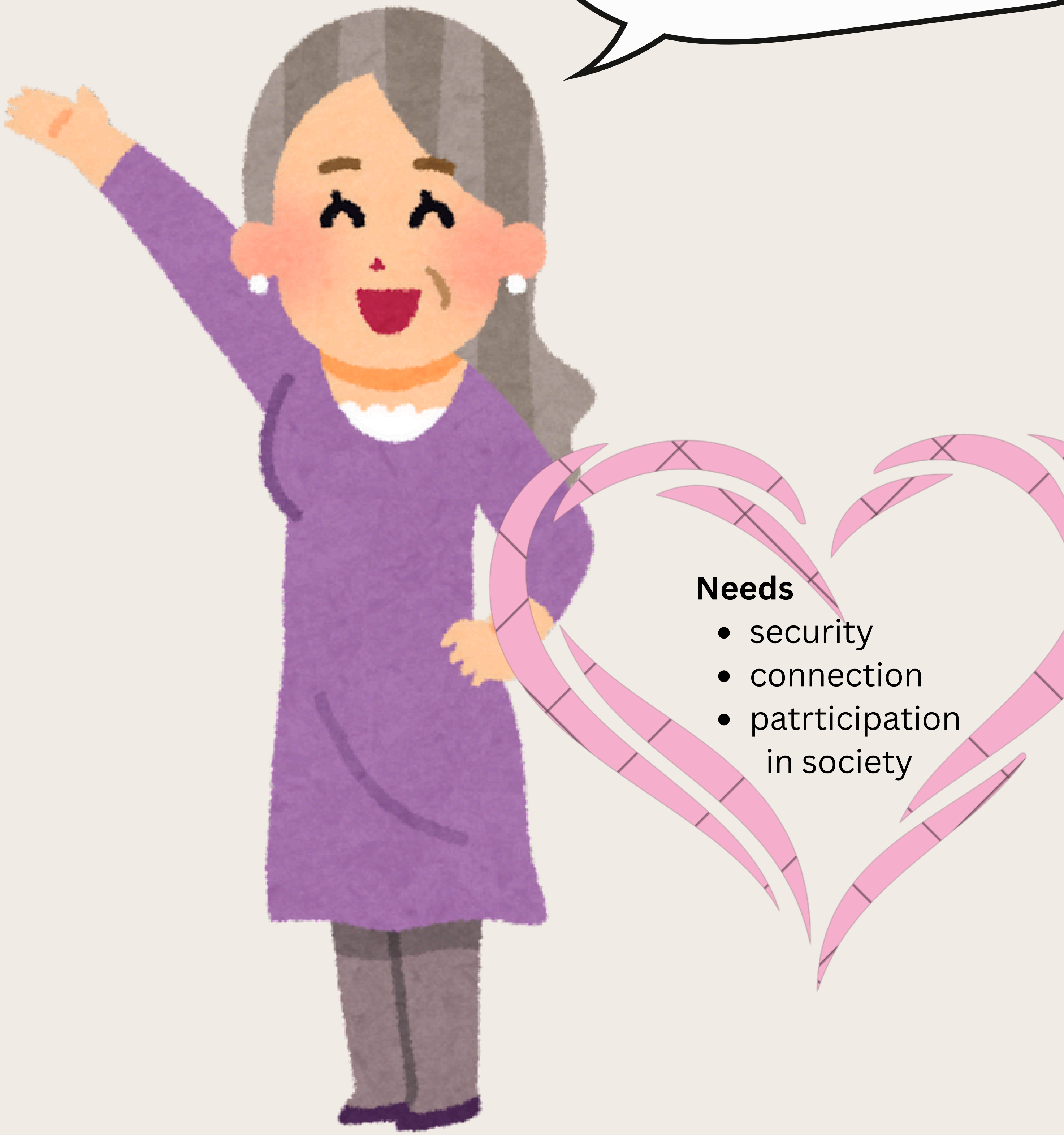
Fears

- loneliness
- disconnection
- fear of isolation

Hopes

- to feel less lonely
- to feel less disconected

I’m Ana Maria
Senior Citizen,
Grandmother

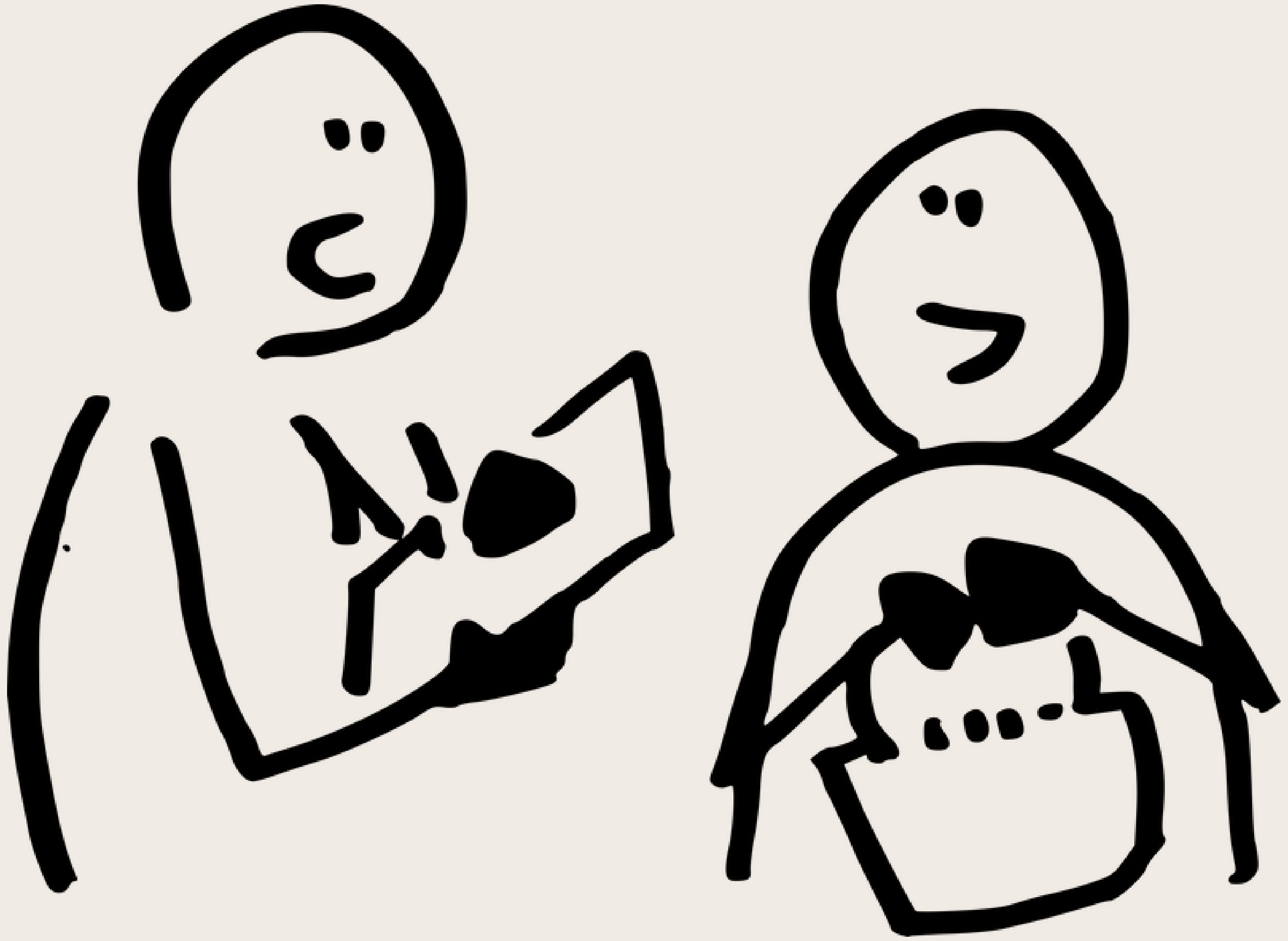


Needs

- security
- connection
- patrticipation in society

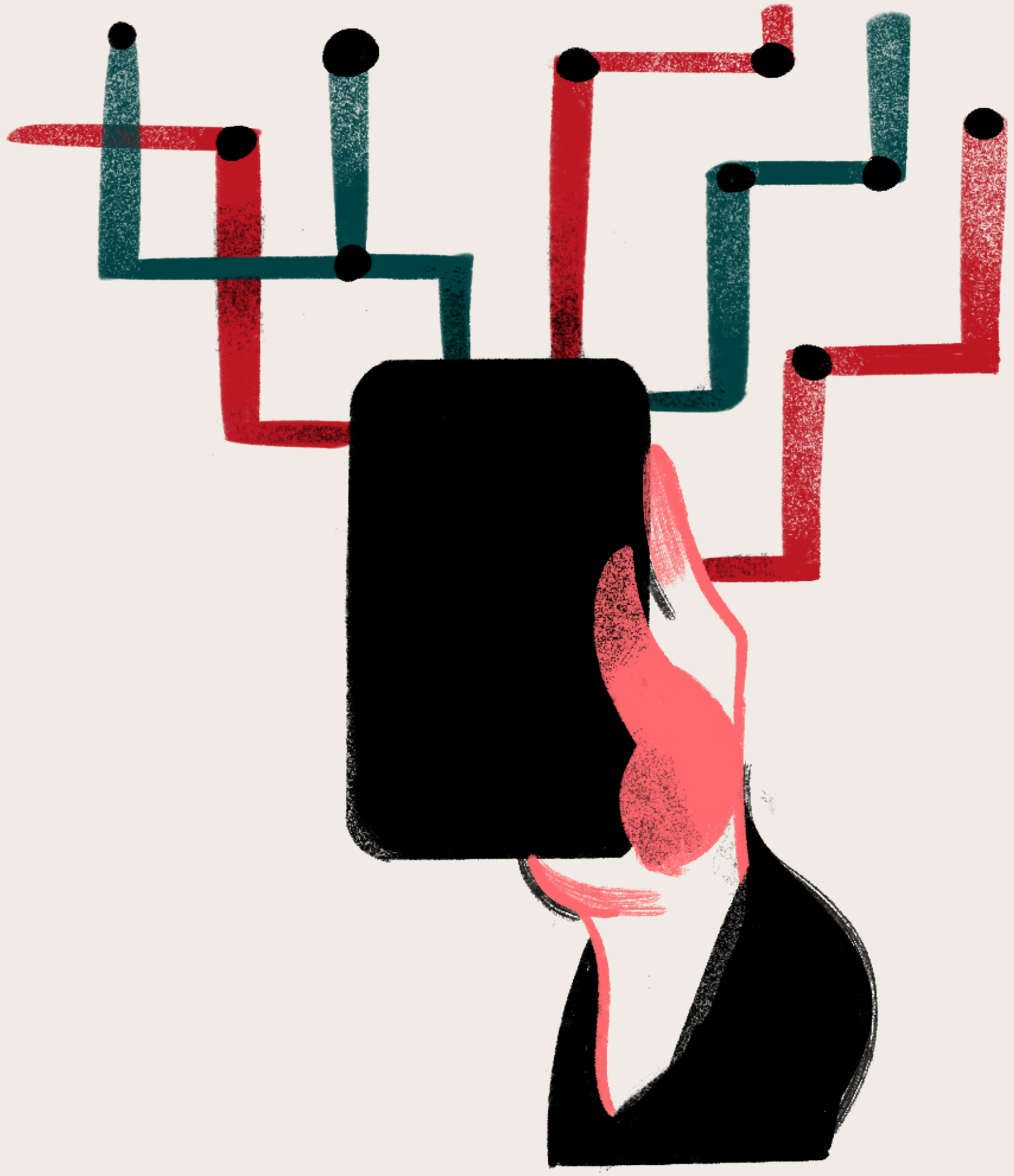
TARGET GROUP: THINGS TO CONSIDER

- rural vs urban gaps
- general opinion on technology
- different resources
- social support system
- different actual needs / practical needs
- individual skill level: general knowledge vs no knowledge
- etc... every individual is different, even with similarities.



WHAT IS OUR VISION?

A world where disadvantages of older citizens do not matter, because they are educated on how to safely go on their tech journey.

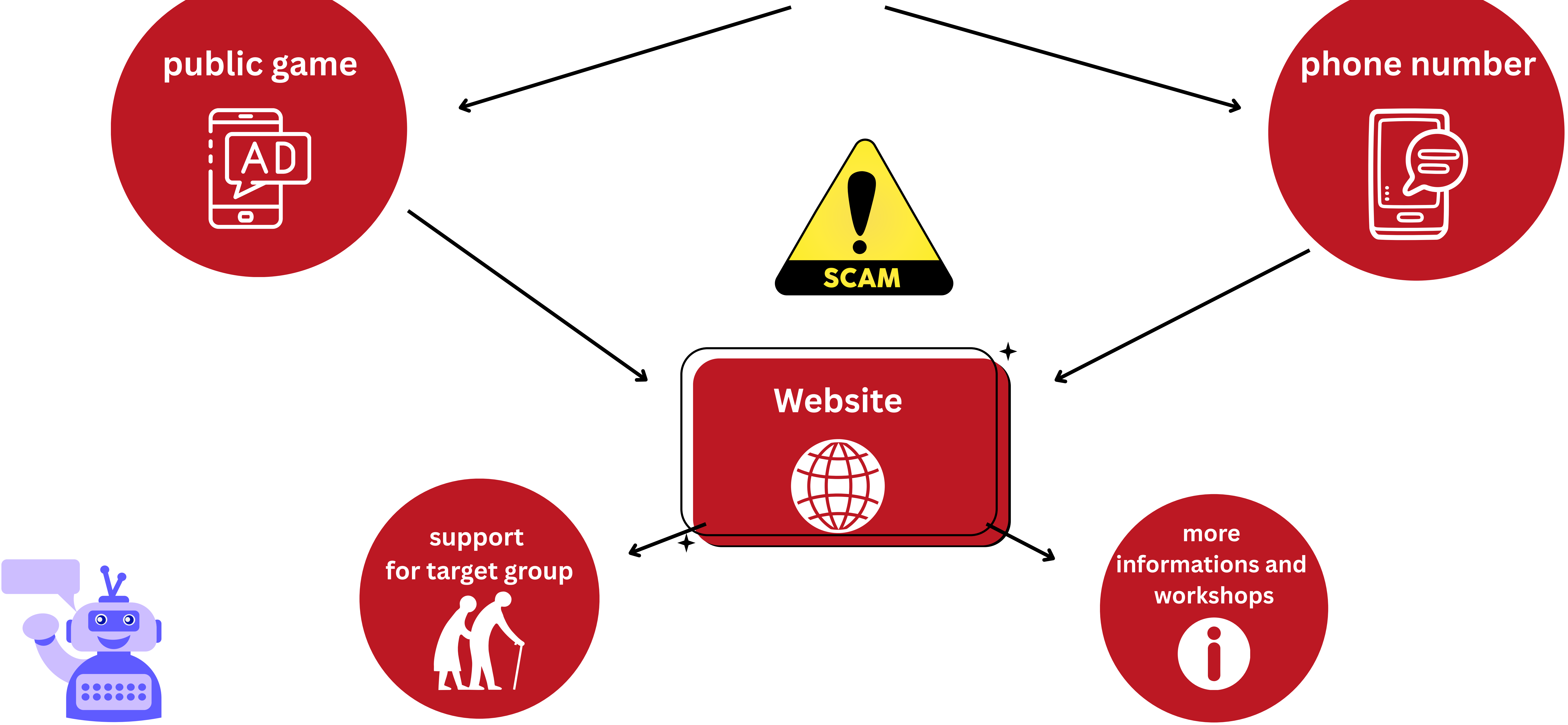


WHAT IS OUR MISSON?

Reduce scams on older people in Europe by 2030.

Offer sustainable education for elderly people to safely traverse the digital world and have better participation chances in society and their social circles.

SENIOR SECTECH



public game

phone number

SCAM

Website

support for target group

more informations and workshops

www.SenlorSecTech.de
Home
Common Scams
Hotline
Workshops & Resources
Contact
SENIOR
SECTECH
You have
been scamed!
SCAM

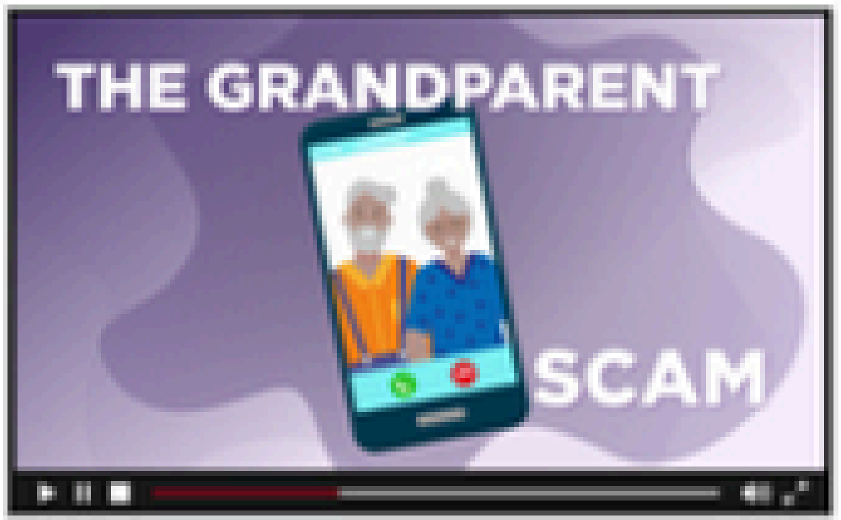
www.SeniorSecTech.de

Home | Common Scams | Hotline | Workshops & Resources | Contact

COMMON SCAMS

1. Health Insurance/Health Care Scams

2.Grandparent Scam



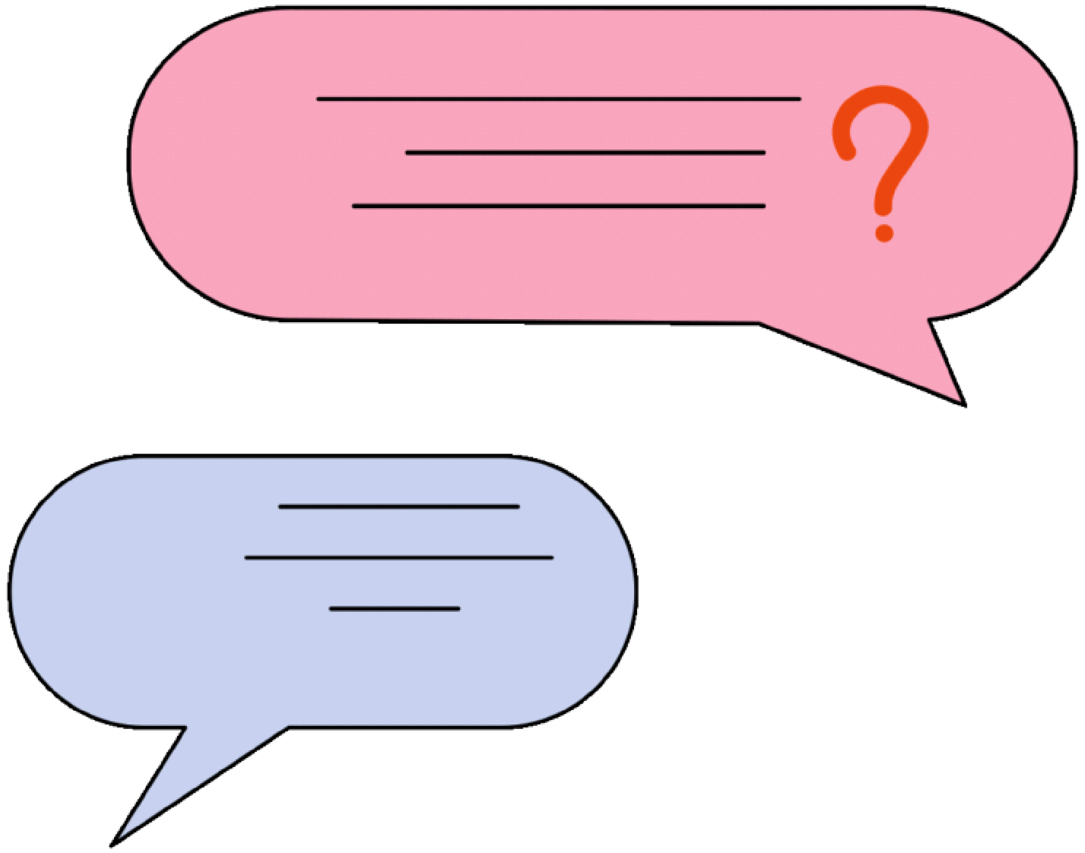
3. Social Security Scams

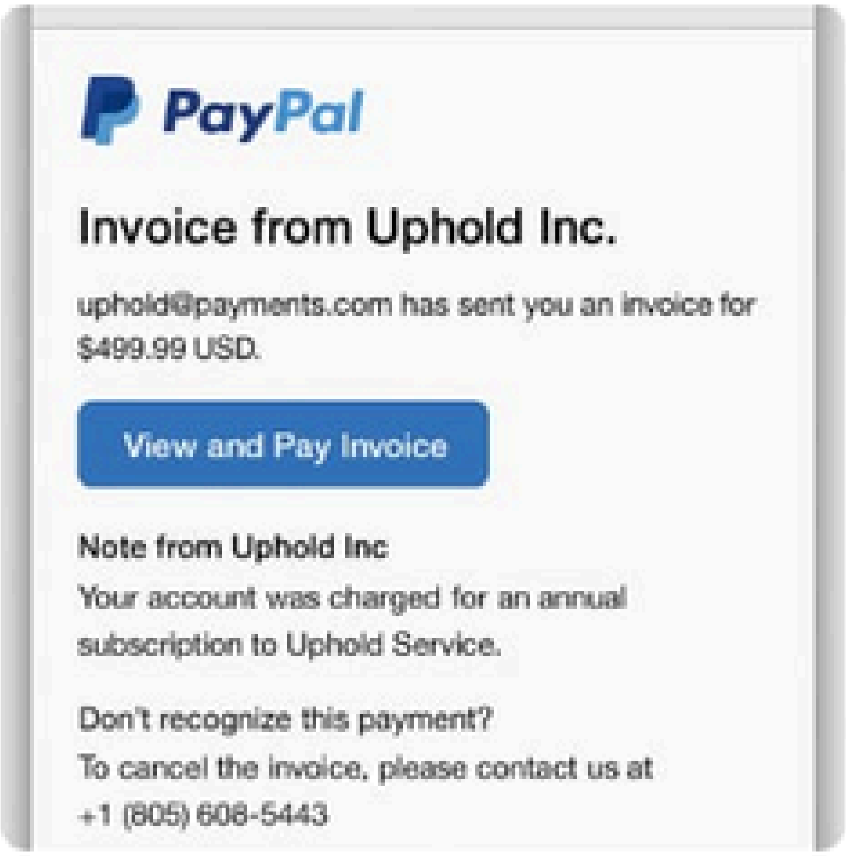
4. Phishing Emails

www.SeniorSecTech.de

Home | Common Scams | Hotline | Workshops & Resources | Contact

HOTLINE





PayPal

Invoice from Uphold Inc.

uphold@payments.com has sent you an invoice for $499.99 USD.

Note from Uphold Inc
Your account was charged for an annual subscription to Uphold Service.

Don't recognize this payment?
To cancel the invoice, please contact us at +1 (805) 608-5443

Is this a scam?

SENIOR SECTECH

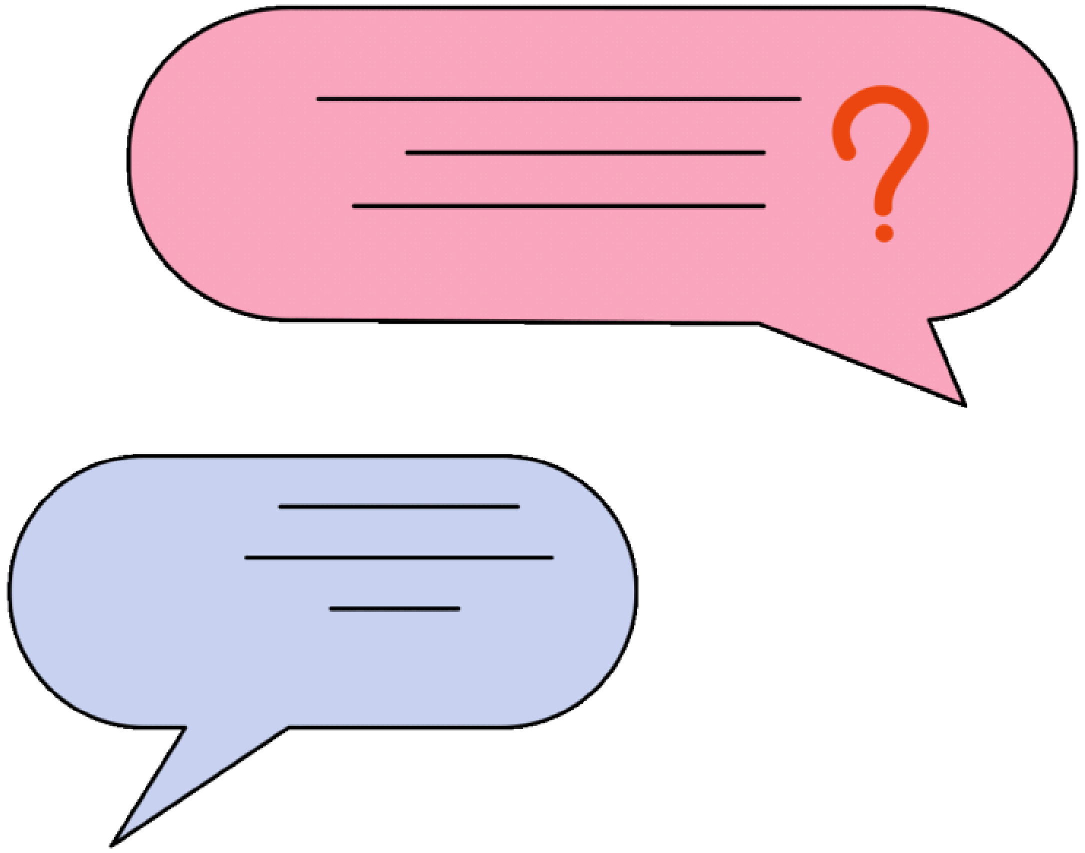
Yes — this looks like a **scam**, and here's why:

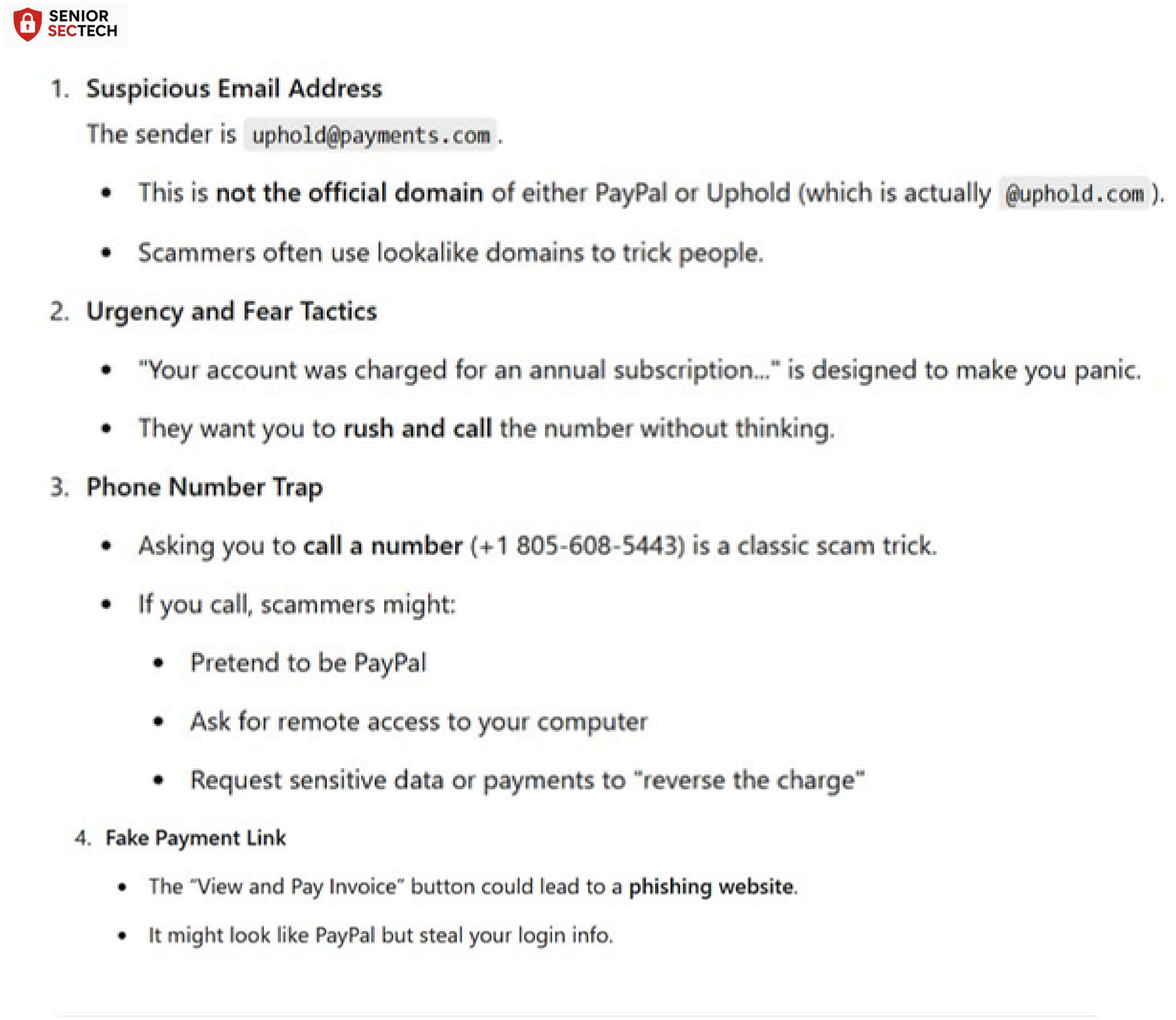
SENIOR SECTECH

www.SeniorSecTech.de

Home Common Scams Hotline Workshops & Resources Contact

HOTLINE





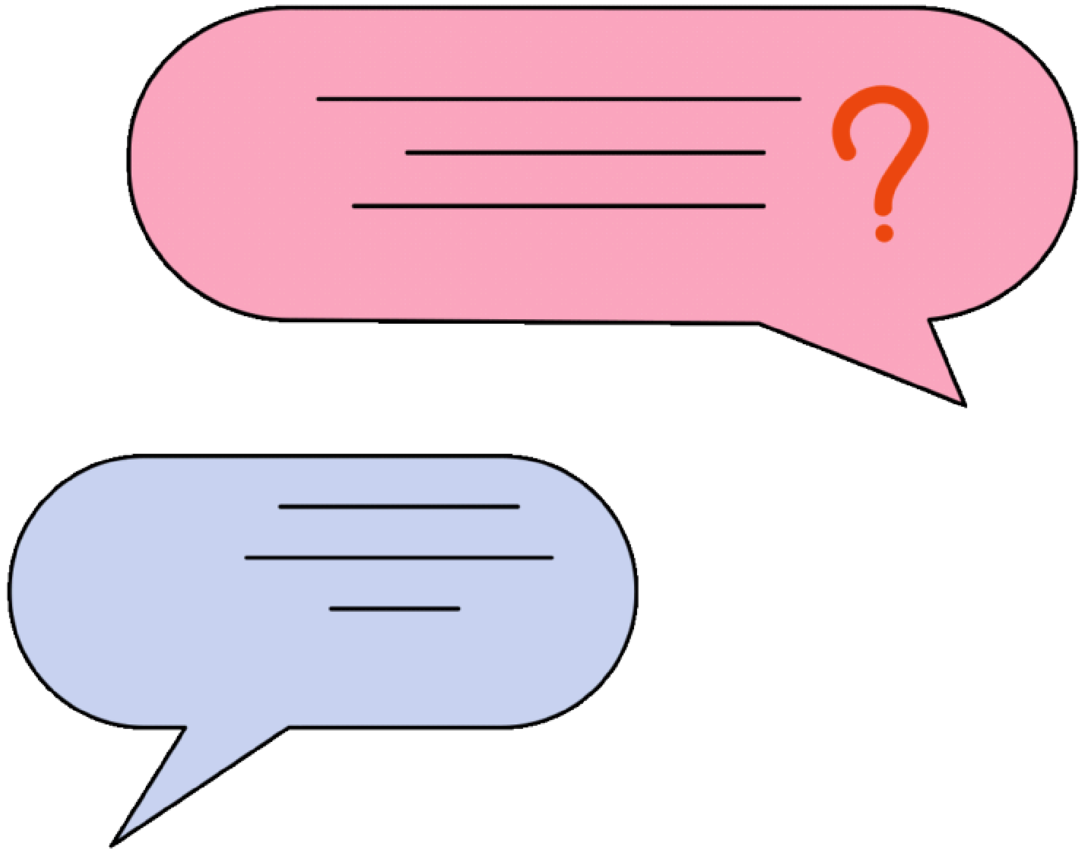
SENIOR SECTECH

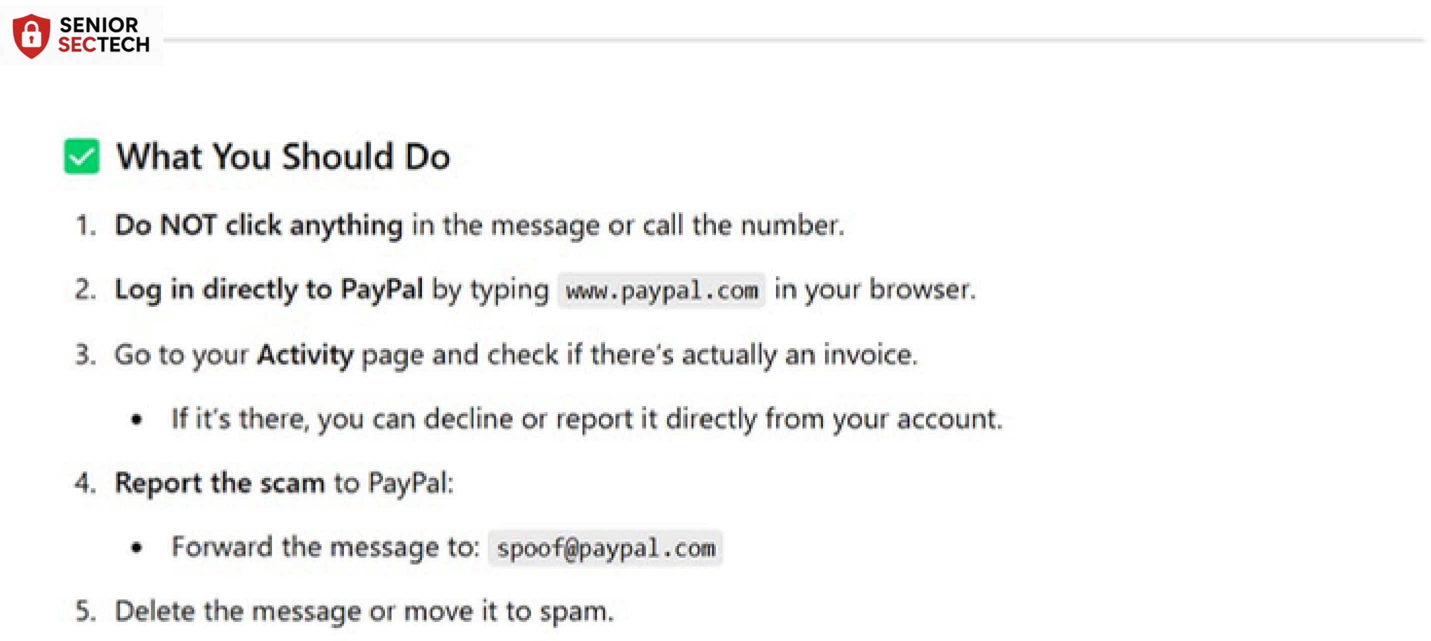
1. **Suspicious Email Address**
   The sender is `uphold@payments.com`.
   - This is **not the official domain** of either PayPal or Uphold (which is actually `@uphold.com`).
   - Scammers often use lookalike domains to trick people.
2. **Urgency and Fear Tactics**
   - "Your account was charged for an annual subscription..." is designed to make you panic.
   - They want you to **rush and call** the number without thinking.
3. **Phone Number Trap**
   - Asking you to **call a number** (+1 805-608-5443) is a classic scam trick.
   - If you call, scammers might:
     - Pretend to be PayPal
     - Ask for remote access to your computer
     - Request sensitive data or payments to "reverse the charge"
4. **Fake Payment Link**
   - The "View and Pay Invoice" button could lead to a **phishing website**.
   - It might look like PayPal but steal your login info.

www.SeniorSecTech.de

Home | Common Scams | Hotline | Workshops & Resources | Contact

HOTLINE





✅ What You Should Do

1. **Do NOT click anything** in the message or call the number.
2. **Log in directly to PayPal** by typing `www.paypal.com` in your browser.
3. Go to your **Activity** page and check if there's actually an invoice.
   - If it's there, you can decline or report it directly from your account.
4. **Report the scam** to PayPal:
   - Forward the message to: `spoof@paypal.com`
5. Delete the message or move it to spam.

www.SenIorSecTech.de

Home | Common Scams | Hotline | **Workshops & Resources** | Contact

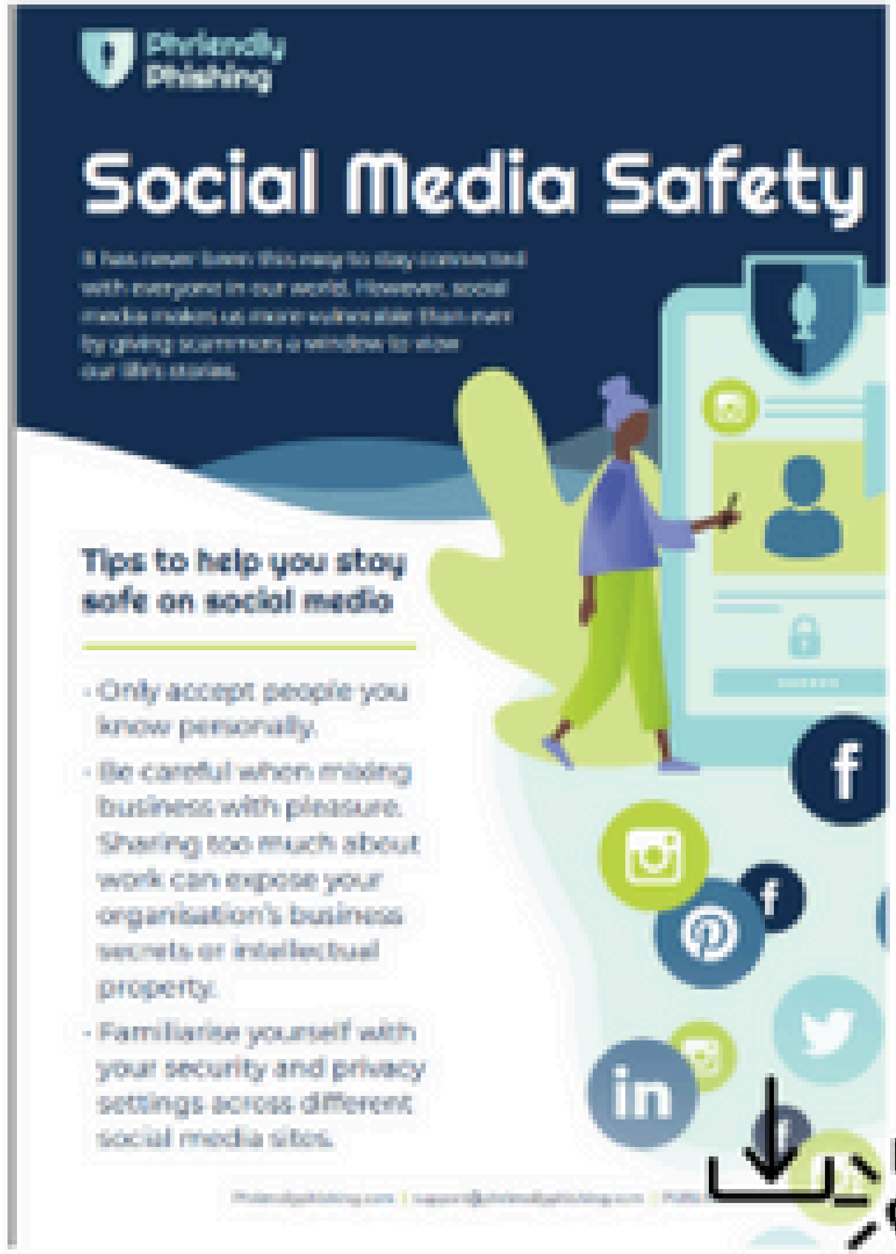
WORKSHOPS & RESOURCES

Workshops

Phising Mail

Cybersecurity Awarness

More Informations



Phriendly Phishing

Social Media Safety

It has never been this easy to stay connected with everyone in our world. However, social media makes us more vulnerable than ever by giving scammers a window to view our life's stories.

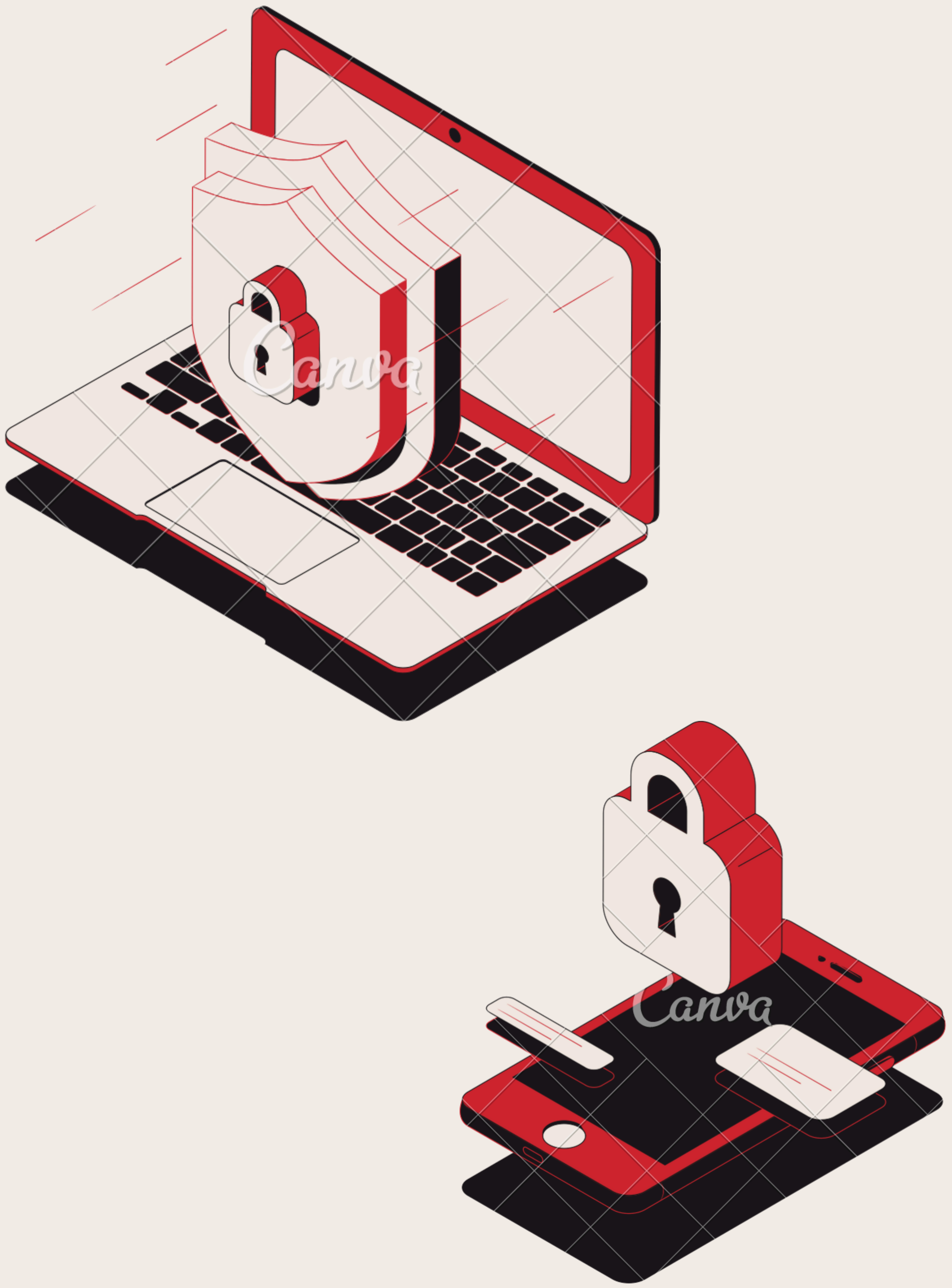
Tips to help you stay safe on social media

- Only accept people you know personally.
- Be careful when mixing business with pleasure. Sharing too much about work can expose your organisation's business secrets or intellectual property.
- Familiarise yourself with your security and privacy settings across different social media sites.

[illegible]

OUR GOAL...

Awareness. Education. Security.



THANK YOU FOR YOUR ATTENTION!

STAY SAFE! 🥰