Social Engineering Awareness

Dr. Mehmet Ali YALÇINKAYA

Kırşehir Ahi Evran University

Department of Computer Engineering

mehmetyalcinkaya@ahievran.edu.tr

Training Agenda : Phase 1 – Understanding Social Engineering Attacks

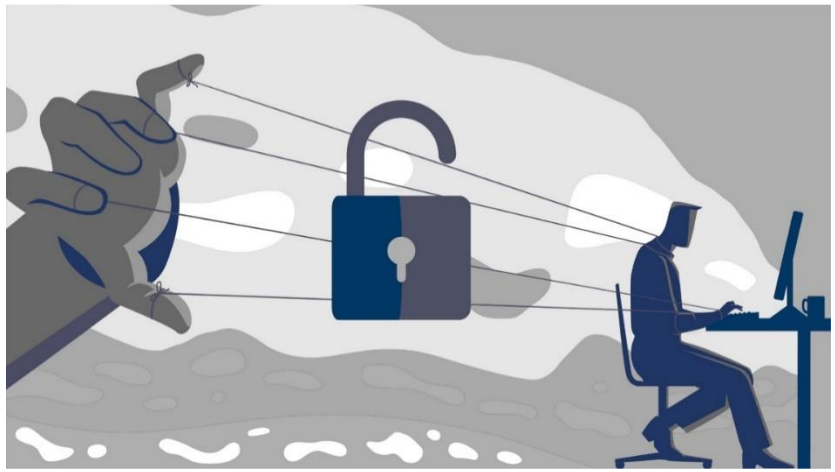
1. **Introduction to Social Engineering**
2. **Why Social Engineering Matters: The Human Factor in Cybersecurity**
3. **Types of Social Engineering Attacks**
   - Phishing and Spear Phishing
   - Smishing and Vishing
   - Baiting
   - Pretexting
   - Shoulder Surfing
4. **Psychological Manipulation Techniques**
   - Authority
   - Urgency
   - Curiosity
   - Fear
5. **Tools and Methods Used by Attackers**
   - Phishing Kits and Fake Login Pages
   - SMS and VoIP Spoofing Tools for Smishing and Vishing
   - USB HID Devices for Baiting Attacks
   - Fake Profiles, Caller ID Spoofing, and OSINT Tools for Pretexting
   - Hidden Cameras and Technical Aids for Shoulder Surfing
7. **Preventive Measures and Best Practices**

Training Agenda : Phase 2 – Training the Trainers

1. **Principles of Adult Learning**
   - Characteristics of Learners Over 50
   - Effective Communication Strategies
   - Accessibility Guidelines for 50+ Learners
2. **Simplifying Complex Cybersecurity Concepts**
   - Using Analogies and Everyday Examples
   - Visual and Storytelling Techniques
3. **Designing Training Materials**
   - Effective Slide Design
   - Brochures, Posters, and Visual Aids
4. **Measuring Learning Outcomes**
   - Pre-test & Post-test
   - Mini Quizzes & Scenarios
   - Feedback Techniques
5. **Key Messages for Older Adults**
   - How to Identify Phishing Emails and SMS
   - Safe Use of Public Wi-Fi and Mobile Applications
   - Importance of Strong Passwords and Two-Factor Authentication
6. **Cultural Considerations in Cybersecurity Awareness Training**
7. **Final Wrap-Up**

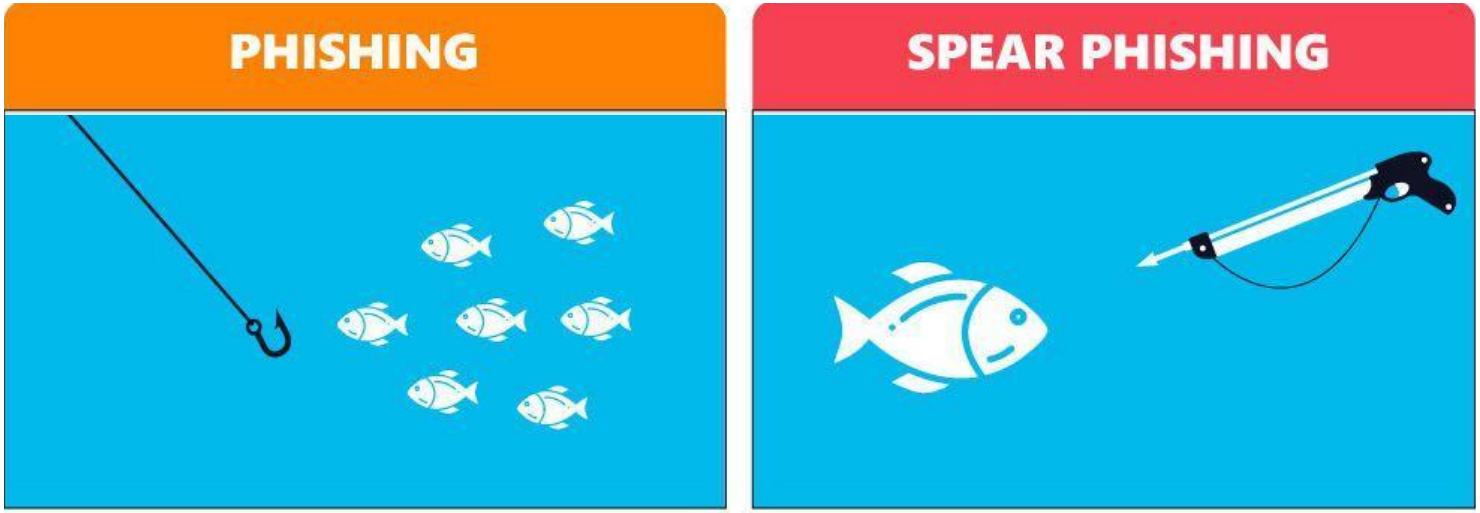
Phase 1: Understanding Social Engineering Attacks

- What is Social Engineering?
  - ✔ A non-technical attack method
  - ✔ Exploiting human psychology instead of system vulnerabilities
  - ✔ Manipulation through trust, fear, curiosity, or urgency
  - ✔ The human factor as the weakest link in cybersecurity
- Why is it Important?
  - ✔ Technology improves, but humans remain vulnerable
  - ✔ A single mistake can compromise an entire system
  - ✔ Social engineering is behind many large-scale cyberattacks



- Humans as the Weakest Link
  - ✔ Advanced technologies protect systems, but not people
  - ✔ One careless click can bypass the strongest defenses
  - ✔ Attackers prefer exploiting human behavior
- Impact of Human Errors
  - ✔ Phishing emails → stolen credentials
  - ✔ Phone scams → leaked sensitive information
  - ✔ Social media manipulation → identity theft, data leaks
- Key Point
  - ✔ Cybersecurity is not only about technology—it is about people.

- Phishing & Spear Phishing
  - ✔ Fraudulent emails are sent to the user.
  - ✔ **Purpose:** To steal passwords, credit cards, or personal information.
  - ✔ **Phishing:** General, mass emails sent to everyone.
  - ✔ **Spear Phishing:** Personalized, targeted attacks



Sent on: Friday, June 23, 2023 11:31:12 AM

To:

Subject: YOUR ACCOUNT IS AT RISK!!

Dear Valued User ,

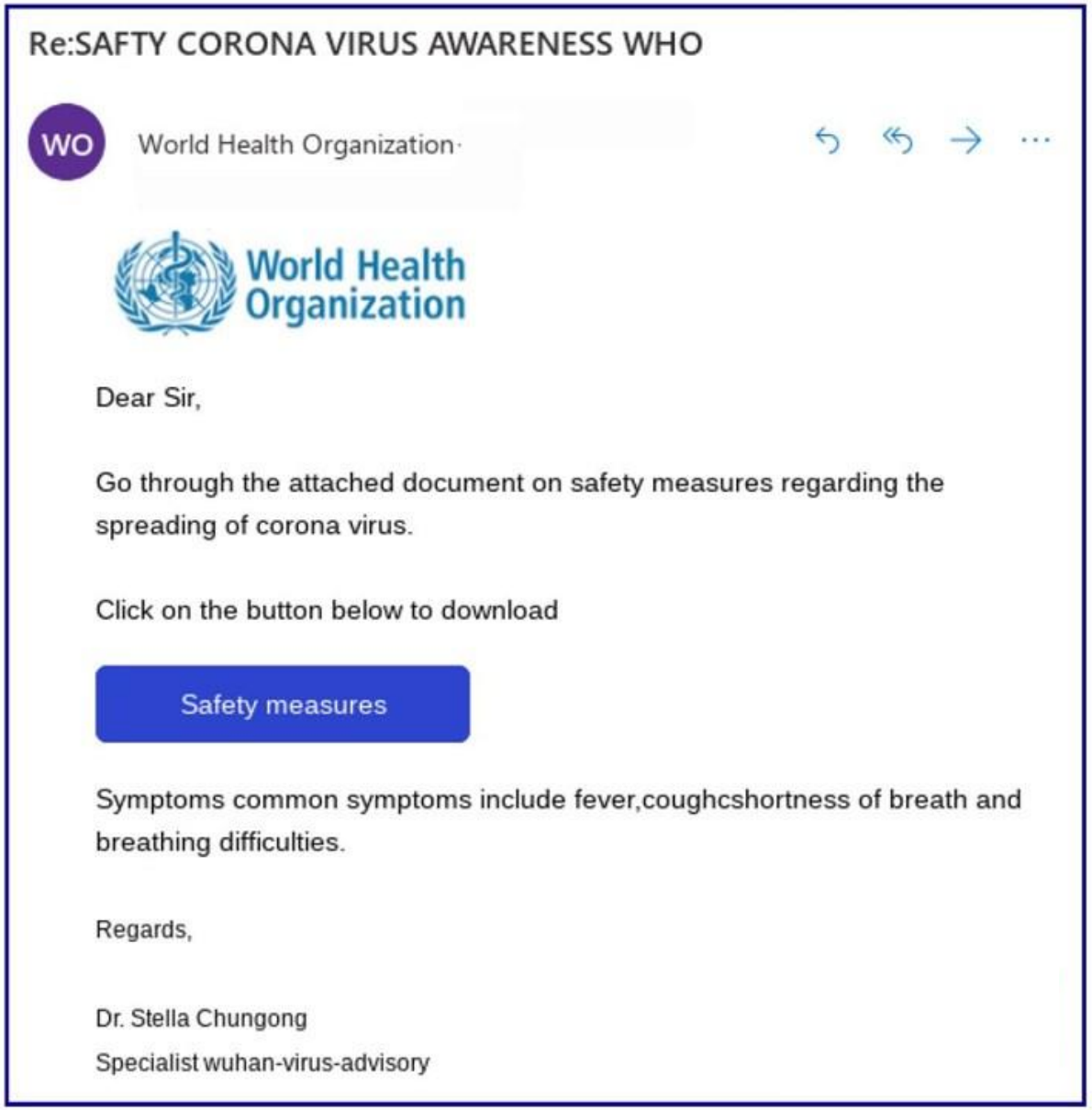
We received a request from you to terminate your Office 365 email due to a dual college/universities account. This process has begun by our administrator. If you did not authorize this action and you have no knowledge of it, you are advised to re-verify your account. Please give us 24 hours to terminate your account if you initiated the request. Failure to re-verify will result in the closure of your account and you will lose all of my files on these 365 accounts.

If this request was made accidentally and you have no knowledge of it, you are advised to copy and paste the URL Below into the address bar of your web browser to fill in the form.

cutt.ly/0wtNi6KO

Failure to Verify will result in the closure of your account.

Iowa State University
IT Helpdesk All Right Reserved.



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization·

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

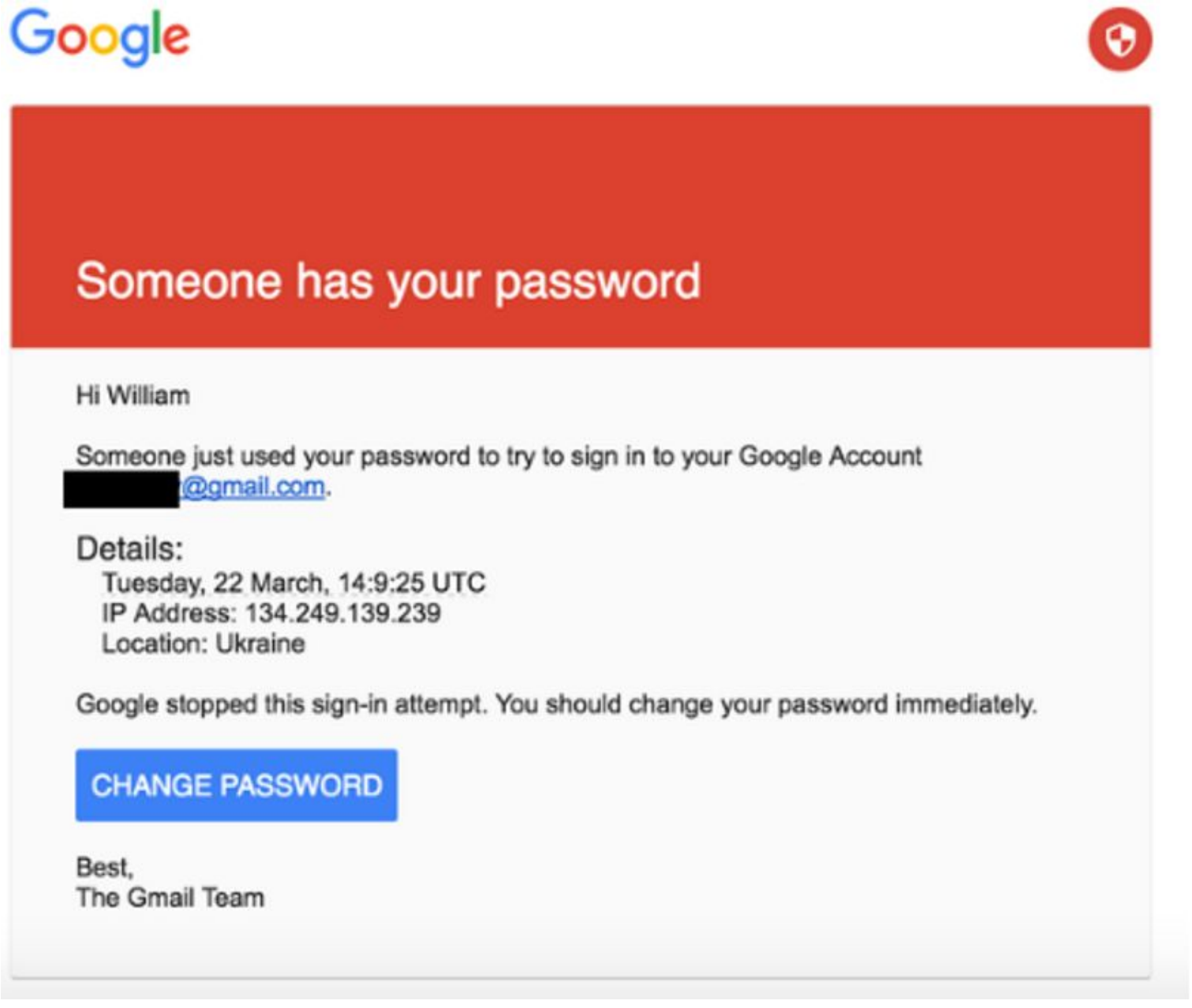
Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong

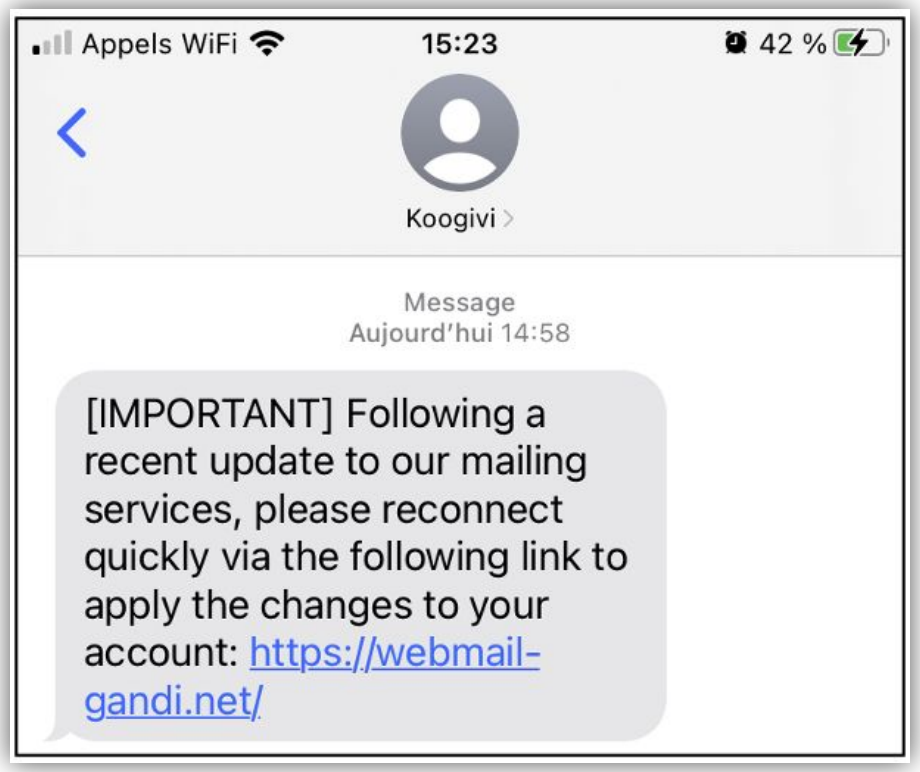
Specialist wuhan-virus-advisory


Google
Someone has your password
Hi William
Someone just used your password to try to sign in to your Google Account
[redacted]@gmail.com.
Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine
Google stopped this sign-in attempt. You should change your password immediately.
CHANGE PASSWORD
Best,
The Gmail Team

Phase 1: Types of Social Engineering Attacks

- Smishing & Vishing
  - ✔ Smishing: fraudulent SMS messages
  - ✔ Vishing: voice-based scams (phone calls)

Phase 1: Types of Social Engineering Attacks- Smishing




AVANOS BLD
Mesaj
Bugün 11:01
Sayin Sanik 11. Agir Ceza Mahkemesi Tarafindan Hukuki Surec Baslatilmistir.Tebligat Yapilmayacaktir. Uygulama Uzerinden Dava Detaylarina Erisebilirsiniz fffutu.re/e-adalet B331
DOLANDIRICILARA DİKKAT!
SMS ile gelen "Sayın Sanık 11. Ağır Ceza Mahkemesi Tarafından Hukuki Süreç Başlatılmıştır. Tebligat Yapılmayacaktır. Uygulama Üzerinden Dava Detaylarına Erişebilirsiniz fffutu.re/e-adalet" mesajına itimat etmeyiniz.
KIRŞEHİR
BELEDİYESİ
1870

- Baiting
  - ✔ Luring victims with free items (USB sticks, downloads, etc.)

"İnat Box" kullananların banka hesapları boşaltıldı! 15 milyonluk vurgun

30 Ağustos 2025 14:29 Güncelleme: 15:17

İnternet üzerinden ücretli dizi, film ve spor müsabakalarını yasa dışı şekilde yayınlayan "İnat Box" isimli uygulamada, 46 kişinin banka hesaplarından toplam 14 milyon 714 bin 354 lira çaldığı tespit edildi. Düzenlenen operasyonda gözaltına alınan 43 şüpheliden 27'si tutuklandı.

- Pretexting
  - ✔ Fake identity or fabricated story to gain trust

Hi Robert,

I need you to make a payment today, Please let me know if you are available so I can forward you the beneficiary's details.

Regards,
[Name]
Chief Executive Officer
Email:
Website: [Company Website]

Phase 1: Types of Social Engineering Attacks- Shoulder Surfing

- Shoulder Surfing
  - ✔ Directly observing someone's screen or keystrokes

The Brussels Times

Up to 48 months in jail for shoulder surfing

Monday 23 June 2025

By The Brussels Times with Belga

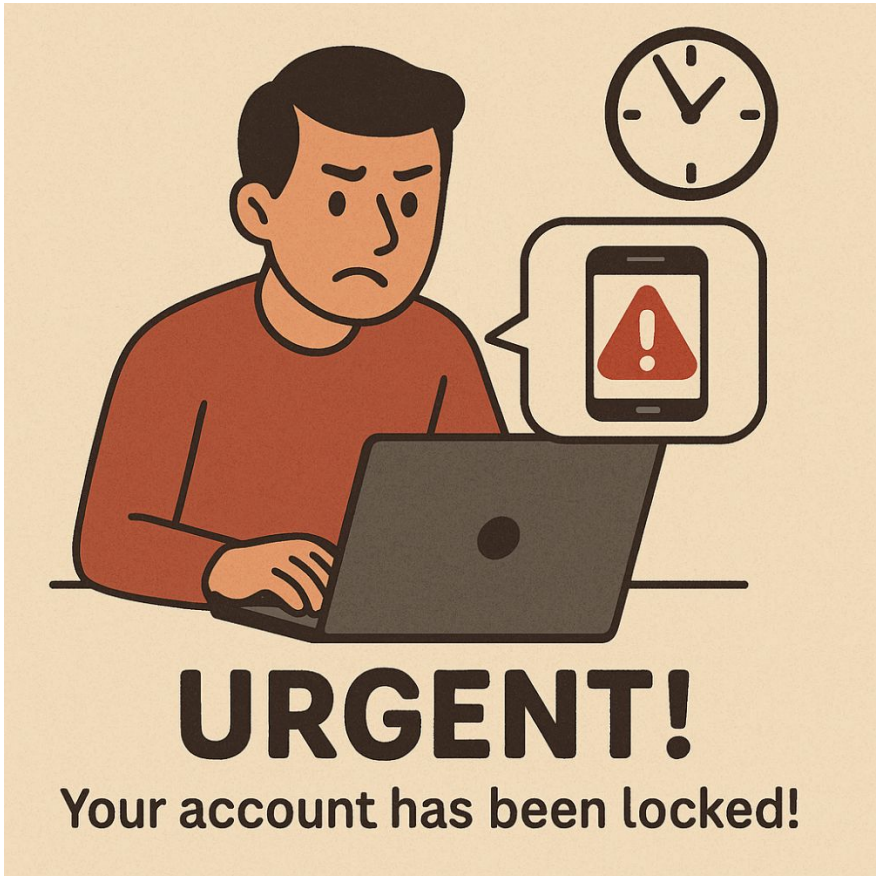
© Bench Accounting via Unsplash

Two French nationals have been sentenced to 48 months in prison, with 37 months to be served, by the Bruges Correctional Court for around fifty thefts.

The accused used a method known as "shoulder surfing" to obtain PIN codes by watching over their victims' shoulders before stealing their bank cards.

- Authority
  - ✔ Attackers pose as trusted figures (banks, police, IT staff)
  - ✔ People tend to obey authority without questioning

- Urgency
  - ✔ Messages create a false sense of time pressure
  - ✔ Victims act quickly without verifying



- Curiosity
  - ✔ Enticing links or files (“See who viewed your profile”)
  - ✔ Exploits natural human interest

- Fear
  - ✔ Threats of account closure, legal action, or financial loss
  - ✔ Victims panic and comply immediately

Purpose: In the previous section, we defined attack types (Types of Social Engineering Attacks) from the victim's perspective. In this section, we explain which tools and methods attackers use to create and execute those same attacks.

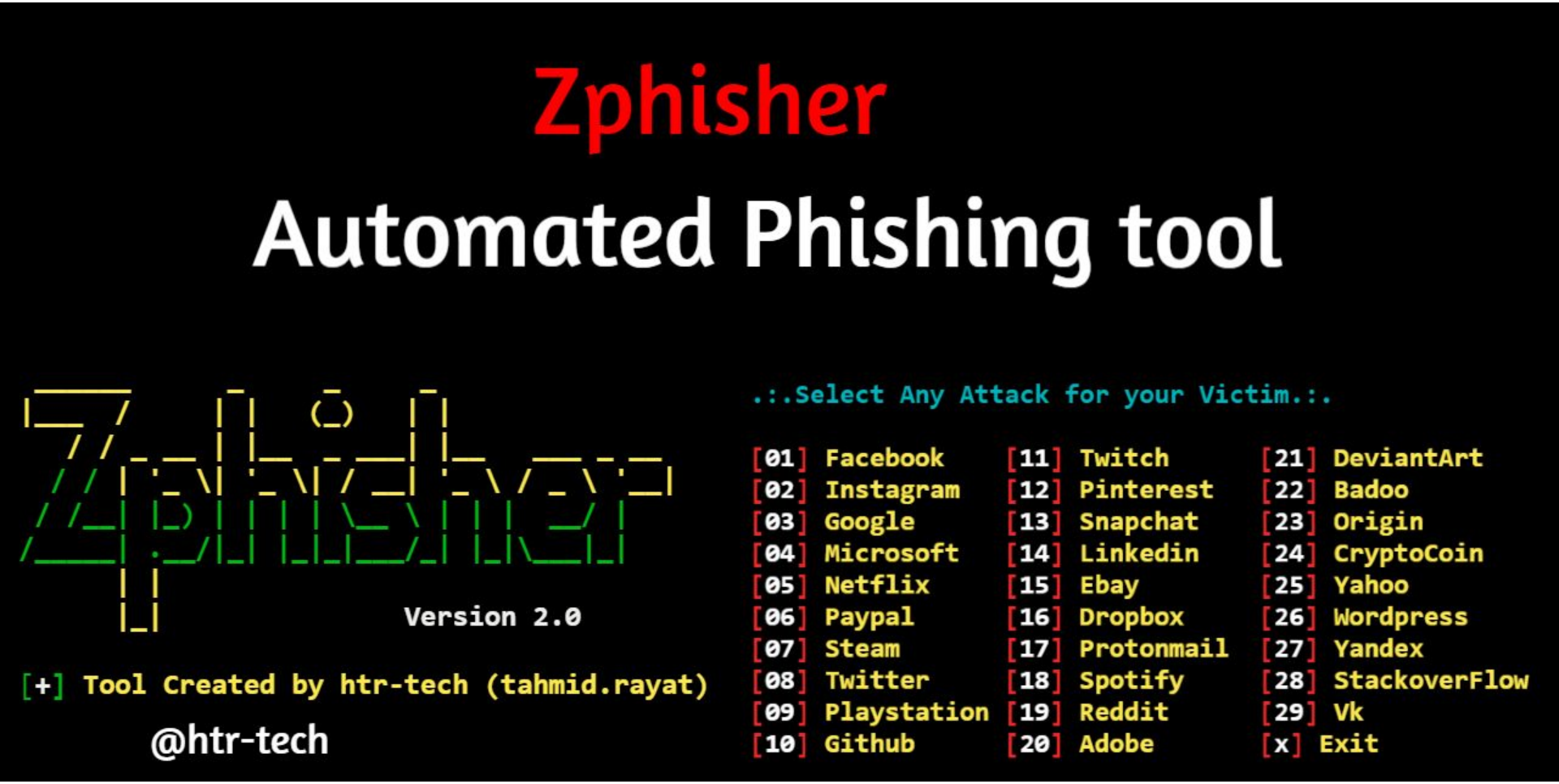
- **Topics to be covered:**
  - ✔ Phishing Kits and Fake Login Pages
  - ✔ SMS and VoIP Spoofing Tools for Smishing and Vishing
  - ✔ USB HID Devices for Baiting Attacks
  - ✔ Fake Profiles, Caller ID Spoofing, and OSINT Tools for Pretexting
  - ✔ Hidden Cameras and Technical Aids for Shoulder Surfing
  - ✔ Defensive Measures Against These Tools
- **Expected outcome:**
  - ✔ For each tool: clear answers to "how does it deceive?" and "how can we defend against it?"
  - ✔ A visible connection between attack types (What) and the tools (How)

Phishing Kits

- Can be found on underground forums, darknet markets, or even open GitHub repositories.
- Ready-made templates for popular services (banks, social media platforms, email providers).
- Typically include:
  - ✔ HTML/CSS/JS files: A replica of the original website
  - ✔ PHP/Python scripts: To send captured usernames and passwords to the attacker
  - ✔ Mailing modules: To send phishing emails to victims
  - ✔ Logging system: To store stolen credentials

Well-Known Phishing Kits and Tools

- **16Shop:** Commercial kits targeting Apple, PayPal, Amazon (sold on darknet).
- **Zphisher:** Open-source, automatically generates fake login pages for social media and banking sites.
- **Gophish:** Designed for awareness training, but abused by attackers.
- **HiddenEye:** Linux-based, clones login pages for various platforms.
- **Modlishka / Evilginx2:** Reverse-proxy based kits that can also capture 2FA tokens.


Zphisher
Automated Phishing tool
Version 2.0
[+] Tool Created by htr-tech (tahmid.rayat)
@htr-tech
.:.Select Any Attack for your Victim.:.
[01] Facebook
[02] Instagram
[03] Google
[04] Microsoft
[05] Netflix
[06] Paypal
[07] Steam
[08] Twitter
[09] Playstation
[10] Github
[11] Twitch
[12] Pinterest
[13] Snapchat
[14] Linkedin
[15] Ebay
[16] Dropbox
[17] Protonmail
[18] Spotify
[19] Reddit
[20] Adobe
[21] DeviantArt
[22] Badoo
[23] Origin
[24] CryptoCoin
[25] Yahoo
[26] Wordpress
[27] Yandex
[28] StackoverFlow
[29] Vk
[x] Exit

Phase 1: Tools and Methods Used by Attacker

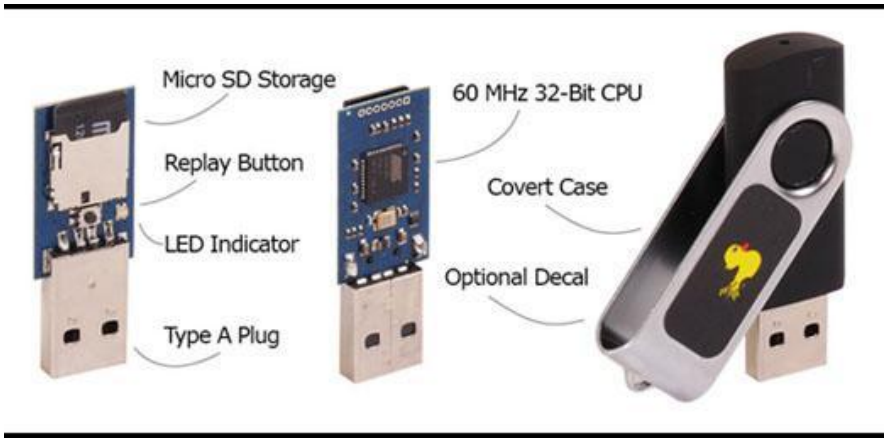
SMS and VoIP Spoofing Tools for Smishing and Vishing

- SMS Gateway Abuse (using APIs to send bulk fake SMS messages)
- SMS Bomber/Sender Kits (for mass texting)
- VoIP Spoofing Software (changing caller ID to impersonate trusted entities)
- AI Voice Cloning (imitating executives or relatives in CEO fraud and emergency scams)

USB HID Devices for Baiting Attacks

- ✔ Appear to be ordinary USB storage drives.
- ✔ When plugged in, they are recognized not as storage, but as a keyboard or mouse.
- ✔ Operating systems trust input devices and accept them automatically.

- **How They Work:**
  - ✔ Instantly execute preloaded commands once connected.
  - ✔ Can open a browser, download malware, create backdoors, or change system settings.
  - ✔ The process happens so fast that the victim often does not notice anything.
- **Connection to Baiting**
  - ✔ Often distributed as promotional gifts, “lost” USB drives, or disguised as genuine storage devices.
  - ✔ Exploit human curiosity or the appeal of free items to make victims plug them in.



Fake Profiles, Caller ID Spoofing, and OSINT Tools for Pretexting

- The attacker creates a believable scenario to deceive the victim.
- Goal: build trust and obtain information or access.

Tools and Methods Used:

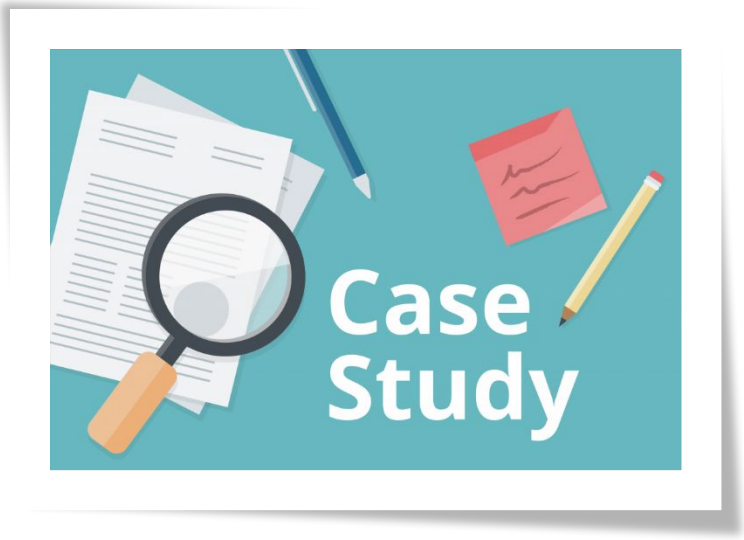
- **Fake Profiles:** Social media accounts (LinkedIn, Facebook, etc.) are created to establish credibility.
- **Caller ID Spoofing:** Phone numbers are manipulated to appear as if calls come from banks, companies, or officials.
- **OSINT Tools**: Tools like Maltego, Recon-ng, and theHarvester are used to gather background information and create more convincing stories.

Phase 1: Tools and Methods Used by Attackers

Hidden Cameras and Technical Aids for Shoulder Surfing

- **Hidden Cameras:** Placed near ATMs or inside offices.
- **Remote Observation:** Using telephoto lenses or binoculars to monitor screens.

- Real-World Case Studies of Social Engineering
  - ✔ Techniques applied in real incidents
  - ✔ Cases from different industries and countries
  - ✔ Lessons learned and awareness gained



Case Description: Using AI-powered deepfake technology, the voice of a senior executive was imitated to issue fraudulent instructions. An employee, trusting what sounded like the CEO's voice, transferred $243,000 to a "trusted supplier" designated by the attackers. The fraud was only discovered afterwards.

Source: https://blog.avast.com/deepfake-voice-fraud-causes-243k-scam

Case Description: In July 2020, attackers used a “phone spear phishing” technique targeting Twitter employees. By tricking staff over the phone, they gained access to internal systems and hijacked high-profile accounts such as Elon Musk and Bill Gates. The compromised accounts were then used to post scam messages promising, “Send Bitcoin and you will get double in return.”

Source: https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking

Case Description: In 2017, a fraudster impersonated a supplier and issued fake invoices to Google and Facebook, successfully extracting $100 million. Despite their advanced technological infrastructures, both companies fell victim to this social manipulation.

Source: https://www.bbc.com/news/technology-39744007

Case Description: Between 2012 and 2016, attackers impersonated IRS and immigration officials, making thousands of phone calls. Victims were threatened with messages like "Pay your tax debt or you will be arrested," enabling the fraudsters to collect hundreds of millions of dollars.

Source:
https://www.nytimes.com/2018/07/23/business/irs-phone-scams-jeff-sessions.html

Key Messages (bullet points):

1. Question suspicious communications → Call back / verify the source
2. Be cautious with links → Don't click, type the URL manually
3. Multi-Factor Authentication (MFA) → Reject suspicious "push" requests
4. QR code and USB safety → Never scan or plug in unknown sources
5. Strong & unique passwords → Use a password manager
6. Keep software & security patches updated
7. Prefer secure connections over public Wi-Fi (VPN/hotspot)
8. Limit personal information sharing (social media/phone calls)
9. Confidential viewing precautions (screen filters, seating arrangements)
10. Incident reporting flow → When, to whom, and how to report

"The first line of defense: the aware user."

Phase 1: Preventive Measures and Best Practices

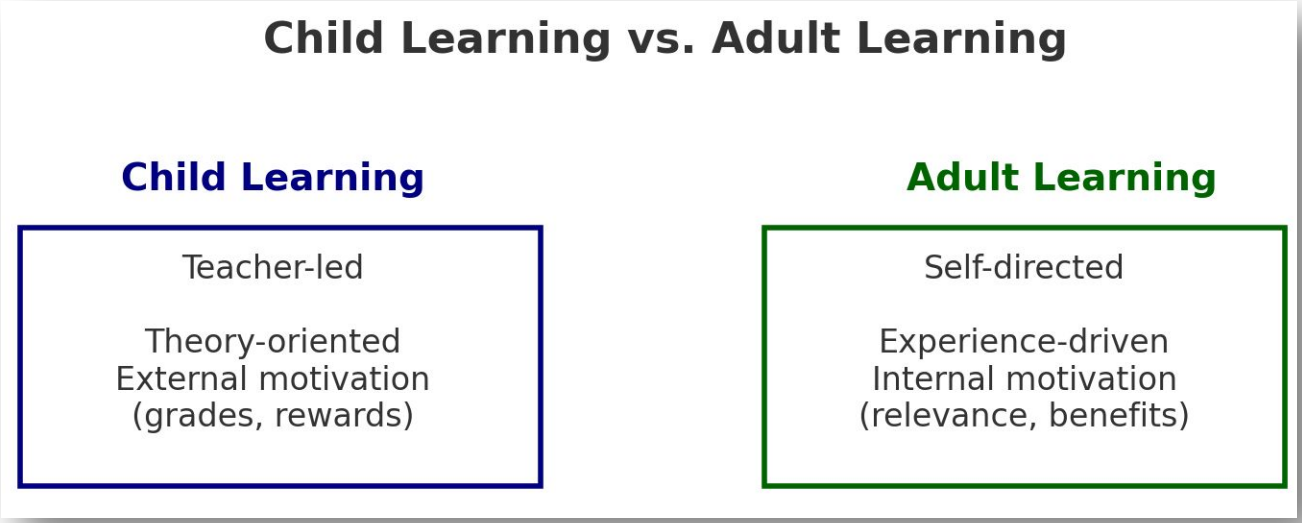
Attack Type	Red Flags (Warning Signs)	Correct Response (Best Practice)
Phishing (E-mail)	Urgency, reward promises, poor grammar, lookalike domains, unexpected attachments	Check sender's domain, hover over links, log in only via official site
Spear Phishing	Personalized details, references to past conversations, unusual requests	Verify identity through another channel; never act without validation
Smishing (SMS)	Bank/delivery/government sender name, short links, urgency	Don't click; use official app or website; call the official number
Vishing (Phone)	Caller pretends to be authority, creates panic, asks for gift cards or money transfer	Hang up; call back via official number; never share sensitive data
Baiting (USB/CD)	Free USBs, CDs, or "free software" offers	Don't connect; hand over to IT/security staff
Pretexting	Fake support/bank agent asking for confidential info	Confirm via official channels; never provide personal or financial data
Shoulder Surfing	Someone observing while typing passwords, visible screens in public	Use a screen filter; shield your keyboard; check surroundings

Phase 2 – Training the Trainers

Training Agenda : Phase 2 – Training the Trainers

1. **Principles of Adult Learning**
    - Characteristics of Learners Over 40
    - Effective Communication Strategies
    - Accessibility Guidelines for 40+ Learners
2. **Simplifying Complex Cybersecurity Concepts**
    - Using Analogies and Everyday Examples
    - Visual and Storytelling Techniques
3. **Designing Training Materials**
    - Effective Slide Design
    - Brochures, Posters, and Visual Aids
4. **Common Barriers**
5. **Measuring Learning Outcomes**
    - Pre-test & Post-test
    - Mini Quizzes & Scenarios
    - Feedback Techniques
6. **Cultural Considerations in Cybersecurity Awareness Training**
7. **Final Wrap-Up**

- Adults are self-directed learners
- Learning is experience-based
- Motivation comes from real-life relevance
- Prefer problem-solving over theory



- Prefer concrete examples & real stories
- May have less confidence with technology
- Value practical benefits over abstract theory
- Learn best with step-by-step guidance
- May require more time for new digital skills

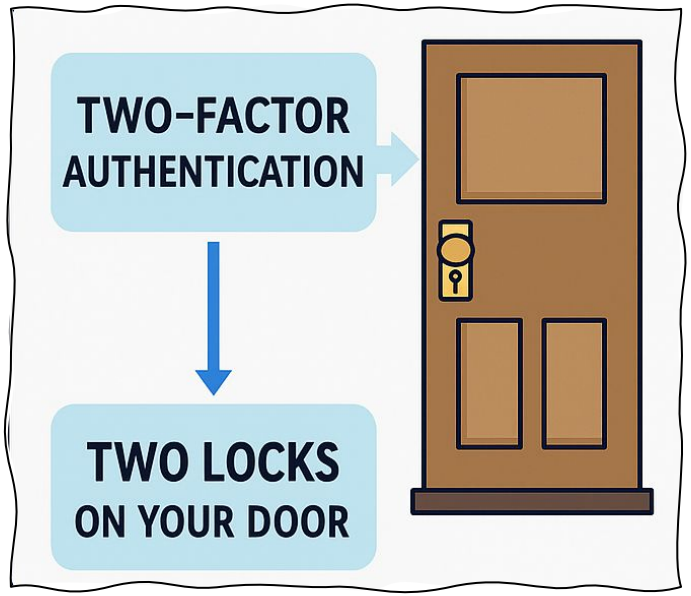
Phase 2: Principles of Adult Learning- Effective Communication Strategies

- Use clear, simple language
- Avoid technical jargon
- Repeat key points for emphasis
- Use questions and interaction
- Highlight “what’s in it for me”

- Large fonts (≥ 24 pt), high contrast colors
- Minimal text per slide
- Use icons & visuals to support text
- Provide printed or digital handouts
- Allow time for repetition and review

- Break down technical terms
- Use familiar comparisons
- Focus on the learner’s daily context
- Keep explanations short & clear

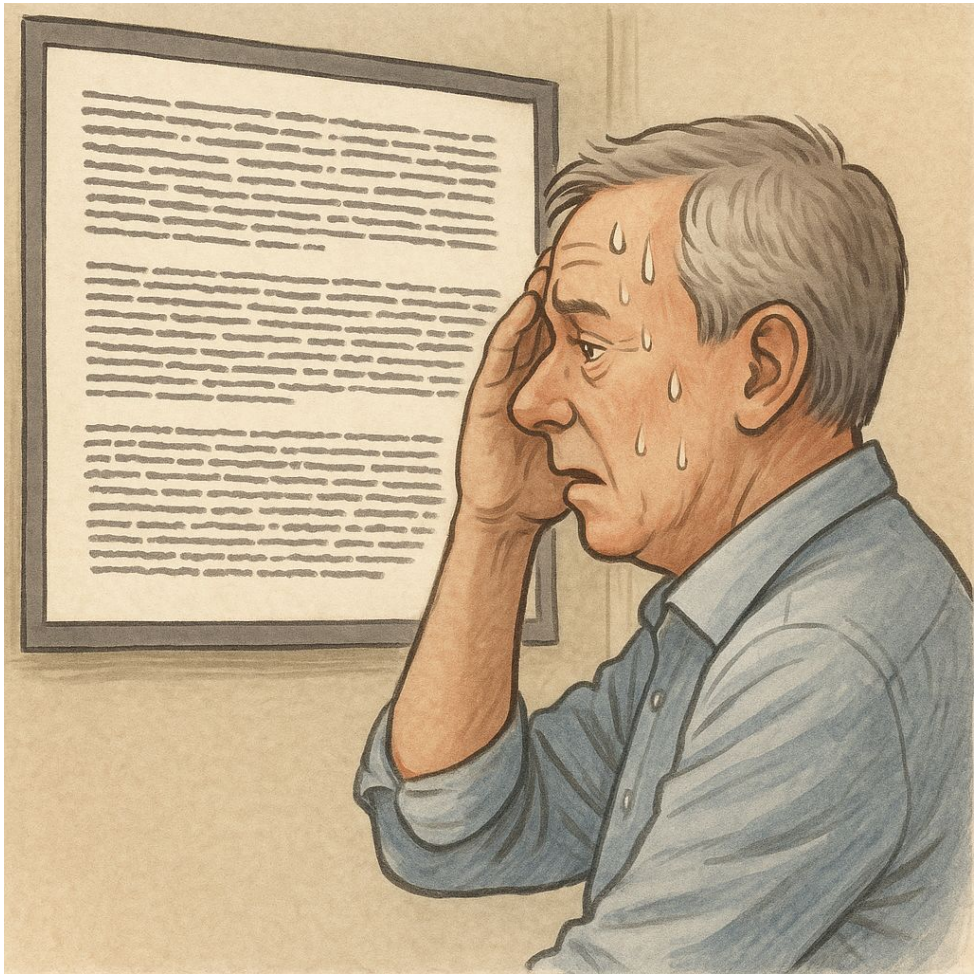
- Phishing → Fishing: baited hook waiting for a victim
- Two-Factor Authentication → Second Lock on a Door
- Firewall → Security Guard at the Gate
- Strong Password → Unique Key for Each Lock
- Public Wi-Fi Risk → Leaving Your Door Unlocked



- Use simple icons and images
- One main message per slide
- Real-life short stories (successes & failures)
- Show “cause & effect” visually

- Materials must be clear, simple, and memorable
- Support learning with both digital and printed resources
- Focus on visual reinforcement

- ✅ Use large fonts and high contrast
- ✅ One main idea per slide
- ✅ Add icons or pictures to support text
- ❌ Avoid clutter and long paragraphs
- ❌ Don’t overload with too much data



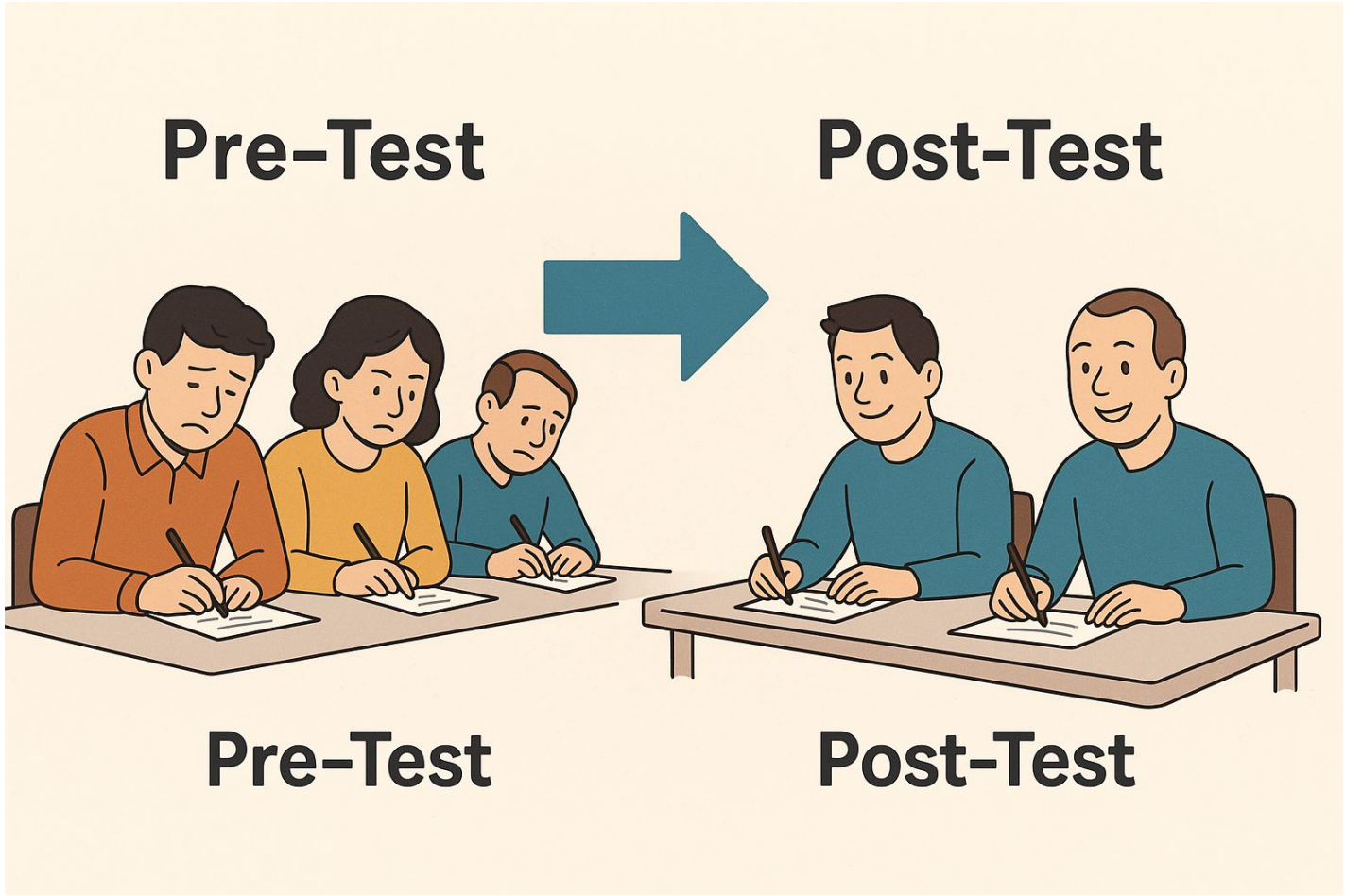
- **Brochures:** step-by-step guides for reference
- **Posters:** reminders in common spaces (offices, schools, community centers)
- **Visual Aids:** flowcharts, checklists, cartoons for easier recall

- Fear of technology
- Memory & attention challenges
- Lack of confidence
- Skepticism

- Safe learning environment
- Repetition & checklists
- Positive feedback
- Real-life relevance

- Why measure? → To check effectiveness of training
- Helps identify what learners understood & what needs reinforcement
- Simple, quick, and non-stressful methods work best for 40+ learners

- **Pre-test:** quick baseline, what participants know before training
- **Post-test:** same/similar questions after training
- Shows improvement, strengthens learning



- Use **2–3 short questions** after each module
- Include **realistic scenarios** → e.g., fake SMS, phishing email screenshot
- Reinforces key lessons & encourages participation

- Short evaluation forms → “What was clear? What was confusing?”
- Quick group discussion → “One thing I learned today…”
- Anonymous feedback → honest insights

Phase 2: Cultural Considerations in Cybersecurity Awareness Training

- Different habits, different risks (banking vs. social media)
- Local language & terminology matter
- Examples must reflect real threats in that country
- Respect cultural norms & communication styles
- Adapt messages to trust channels (government, banks, community centers)

- Kahoot! → Create fun quizzes, test knowledge live
- Spot the Phish Games (various platforms) → Practice identifying phishing e-mails & SMS
  - (ForExample: https://globallearningsystems.com/freecontent/SpotThePhish/story.html)
- Use these tools to:
  - Reinforce learning
  - Keep participants engaged
  - Make cybersecurity awareness memorable

Phase 2: Final Wrap-Up

- Review of Phase 1:
  - ✔ Social engineering types & tactics
  - ✔ Psychological manipulation techniques
  - ✔ Real-world case studies
  - ✔ Preventive measures
- Review of Phase 2:
  - ✔ Adult learning principles & accessibility
  - ✔ Simplifying cybersecurity concepts
  - ✔ Designing effective materials
  - ✔ Measuring learning outcomes
  - ✔ Key security messages for 40+ learners
  - ✔ Cultural adaptation strategies

Thank you for listening