**LA DIFESA PIÙ FORTE È LA PERSONA**

# CLICKFIX: NON FARTI INGANNARE DALLE FINTE SOLUZIONI



Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

Il ClickFix è una tecnica di truffa che spinge le persone a eseguire istruzioni apparentemente utili, ma che possono **infettare** il dispositivo.

COME DIFENDERTI:

1. diffida di **avvisi improvvisi** che segnalano errori e ti spingono ad agire con **urgenza**;

2. non seguire istruzioni online che ti chiedono di eseguire operazioni **insolite** sul dispositivo per risolvere un presunto problema;

3. se **compare** un presunto problema tecnico, chiudi la pagina e utilizza gli strumenti di **assistenza** ufficiali.

**Non cercare scorciatoie:** una soluzione teoricamente utile può trasformarsi in una minaccia per il tuo dispositivo.

**LA DIFESA PIÙ FORTE È LA PERSONA**

# TRUFFE GENERATE DALL'AI: NON FARTI INGANNARE



Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

Email impeccabili o richieste urgenti e credibili? Anche l'**intelligenza artificiale** può nascondere una truffa.

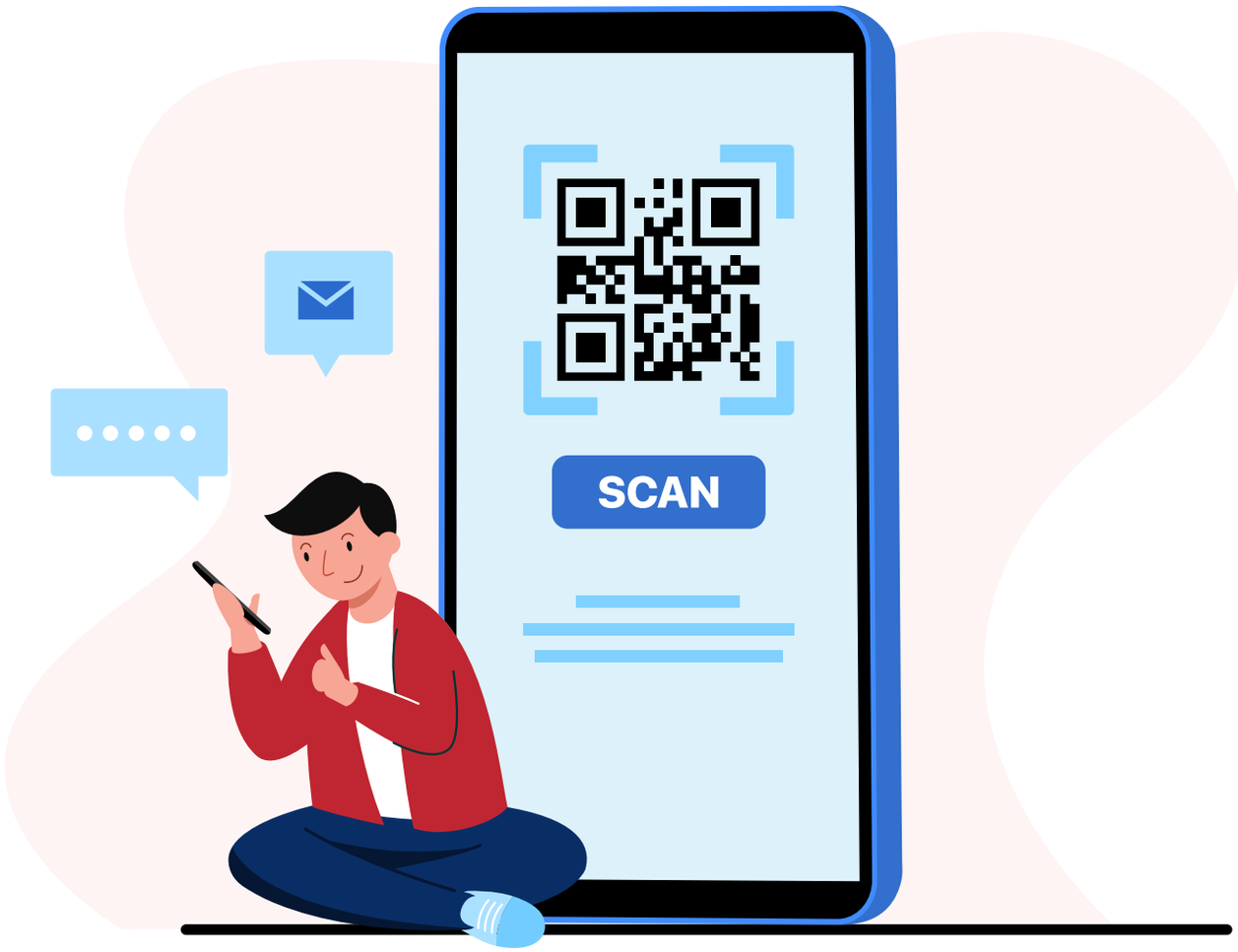
PER PROTEGGERTI:

1. non considerare una voce familiare o un video realistico una **prova certa** di identità;
2. conferma le richieste insolite contattando **direttamente** la persona interessata tramite un recapito **già noto**;
3. **diffida** delle richieste che impongono segretezza, urgenza o procedure fuori dall'ordinario.

La tecnologia evolve, ma la **prudenza** resta la tua miglior difesa.

**LA DIFESA PIÙ FORTE È LA PERSONA**

# QR CODE SOSPETTI: OCCHIO A COSA SCANSIONI




PRIMA DI ACCEDERE A UN ACCOUNT O INSERIRE DATI PERSONALI TRAMITE QR CODE:

1. assicurati che il codice provenga da una **fonte affidabile**;
2. **controlla l'indirizzo** del sito prima di aprire il link o inserire credenziali;
3. evita di scaricare file o installare app suggerite da siti raggiunti tramite QR code **sospetti**.

**Non abbassare la guardia:** anche un QR code può nascondere un rischio.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

**LA DIFESA PIÙ FORTE È LA PERSONA**

# LA TUA SICUREZZA INIZIA DALLA PASSWORD



PROTEGGERE I TUOI ACCOUNT È IL PRIMO PASSO PER LA SICUREZZA DI TUTTI.

1. Evita **parole comuni** o **date di nascita**;

2. scegli invece password **complesse**, **uniche** e possibilmente generate da un password manager autorizzato;

3. non riutilizzare **mai** la stessa password per più servizi.

Per un livello di protezione extra, attiva sempre l'**autenticazione a più fattori** (MFA): un piccolo gesto che impedisce agli estranei di accedere ai tuoi dati anche se conoscono la tua password.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

**THE STRONGEST LAYER IS HUMAN**

# CLICKFIX: DON'T BE FOOLED BY FAKE FIXES!



ClickFix is a scam technique that tricks people into following seemingly helpful instructions that can **infect** their devices.

HERE'S HOW TO PROTECT YOURSELF:

1. be wary of **unexpected alerts** reporting errors and pressuring you to act **urgently**;

2. don't follow online instructions asking you to perform **unusual** actions on your device to fix an alleged problem;

3. if a supposed technical issue **appears**, close the page and use official **support** tools.

**Don't look for shortcuts:**
a solution that seems helpful in theory can turn into a threat to your device.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

**THE STRONGEST LAYER IS HUMAN**

# AI-GENERATED SCAMS: DON'T BE FOOLED!



Flawless emails or urgent, convincing requests? **Artificial intelligence** can also be used to disguise a scam.

HERE'S HOW TO PROTECT YOURSELF:

1. don't assume that a familiar voice or a realistic-looking video is **definitive proof** of someone's identity;
2. verify unusual requests by contacting the person **directly** using contact details you **already know** to be genuine;
3. **be wary** of requests that demand secrecy, create a sense of urgency or involve unusual procedures.

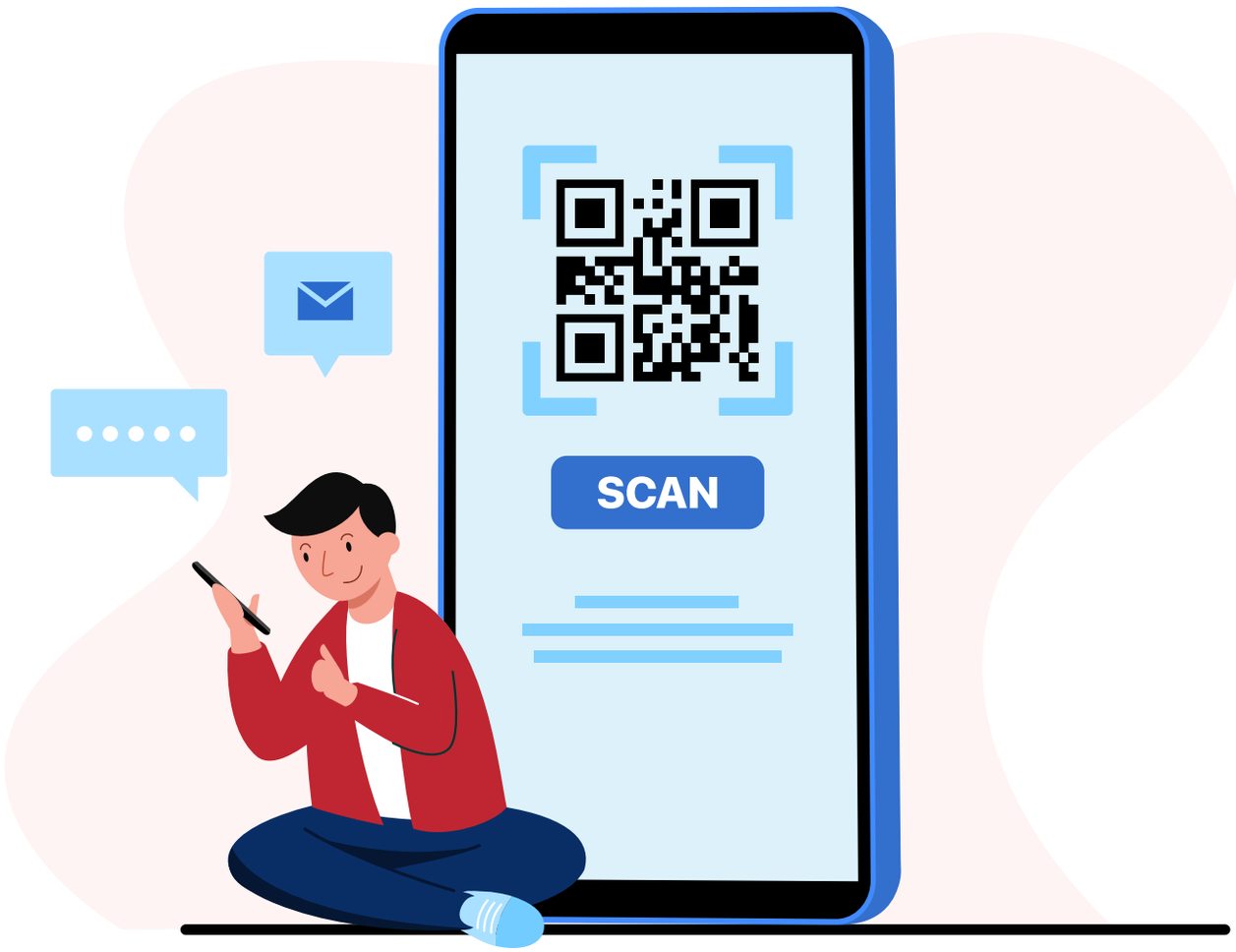
Technology evolves, but **caution** remains your best defence.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

**THE STRONGEST LAYER IS HUMAN**

# SUSPICIOUS QR CODES: WATCH WHAT YOU SCAN!




BEFORE ACCESSING AN ACCOUNT OR ENTERING PERSONAL INFORMATION VIA A QR CODE:

1. make sure the code comes from a **trustworthy source**;

2. **check the website address** before opening the link or entering your login credentials;

3. avoid downloading files or installing apps recommended by websites accessed through **suspicious** QR codes.

**Stay alert:** even a QR code can hide a threat.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik

# THE STRONGEST LAYER IS HUMAN

## YOUR SECURITY STARTS WITH YOUR PASSWORD



PROTECTING YOUR ACCOUNTS IS THE FIRST STEP TOWARDS KEEPING EVERYONE SAFE.

1. Avoid **common words** or **dates of birth**;

2. instead, choose **strong**, **unique** passwords, preferably generated by an approved password manager;

3. **never** reuse the same password across multiple services.

For an extra layer of protection, always enable **multi-factor authentication** (MFA): a simple step that prevents unauthorised people from accessing your data, even if they know your password.

Based on
ENISA (www.enisa.europa.eu)
ACN (www.acn.gov.it)

Image by Freepik