Truffe Informatiche

Come riconoscerle e difendersi

UNITRE

UNIVERSITA' DELLE TRE ETA'

UNITRE SEDE DI ALBANO LAZIALE

INTRODUZIONE

- **Internet, smartphone e servizi online** ci semplificano la vita, ma purtroppo sono anche usati da persone senza scrupoli per truffare.
- Le **truffe informatiche** sono attività criminali che sfruttano computer, smartphone, internet per ingannare le persone e ottenere denaro, dati personali o credenziali di accesso (**password, PIN, codici bancari e altre informazioni**).
- Non colpiscono perché siamo ingenui, ma perché sono studiate per **mettere fretta, creare paura o fingere affidabilità**.

INTRODUZIONE

Questa presentazione ha tre obiettivi:

- **conoscere le truffe più comuni**
- **capire i rischi reali**
- **imparare regole semplici per difendersi**
- **acquisire consapevolezza e non arrendersi di fronte alle truffe**

Le truffe informatiche hanno un nome

- Le truffe **non sono casuali**
- Seguono **schemi precisi e ricorrenti**
- Ogni schema ha **un nome**

Adesso vedremo le truffe una per una

- Per ciascuna tipologia di capiremo:
  - come funziona
  - qual è il rischio
  - come difendersi

Riconoscere il tipo di truffa è un primo passo per difendersi.

Phishing (email e messaggi ingannevoli)

📊 Schema della truffa

- Arriva una **email**
- Sembra della banca, Poste, INPS, Amazon, PayPal
- Chiede di cliccare un link o inserire dati personali

📝 Descrizione

Il messaggio della mail sembra ufficiale ma è falso. Il link porta a un sito che potrebbe sembrare quello vero ma non lo è, e ruba le credenziali di accesso che avete inserito.

Phishing (email e messaggi ingannevoli)

⚠ Rischio

- Furto di password
- Accesso al conto bancario, altro
- Perdita di denaro

Come difendersi

- Le banche **non chiedono dati via email**
- Non cliccare il link ricevuto nella mail. Per accedere alla propria Banca, Poste, INPS, Amazon, PayPal,… **entrare sempre, dal sito ufficiale**
- Controllare errori di lingua o indirizzi strani

Smishing (truffe via SMS)

Schema della truffa

- SMS che si finge un servizio di consegna (SDA, UPS, DHL,o altre ditte di delivery), con messaggi come **“Pacco in arrivo”, “Consegna sospesa”, “Clicca qui per vedere i dettagli”, “ Il tuo pacco è in transito”.**
- Nei messaggi c’è sempre un link da cliccare subito

Descrizione

Il messaggio sembra di un servizio di consegna sembra e sfrutta l’ansia e la fretta. Spesso arriva da numeri sconosciuti.

Smishing (truffe via SMS)

⚠️ Rischio

- Installazione di virus
- Furto di dati personali

🛡️ Come difendersi

- Non cliccare link negli SMS
- Cancellare il messaggio
- Se aspettate una consegna occorre verificare direttamente con il servizio vero del vostro fornitore.

Vishing (truffe telefoniche)

Schema della truffa

- Telefonata da finto operatore di una banca o altro ufficio
- Voce gentile o molto autoritaria
- Sul telefono può comparire un numero che sembra davvero quello della banca
- Richiesta di codici o conferme

(Usano una tecnica chiamata **spoofing del numero,** il numero che compare sul tuo telefono **può essere falsificato,** quindi anche se vedi il numero reale della banca, **non è detto che sia davvero la banca)**

Vishing (truffe telefoniche)

Descrizione

- Il truffatore si finge banca, assistenza tecnica o altro, la voce mette fiducia e nello stesso tempo crea pressione emotiva e mette urgenza.

Rischio

- Accesso ai conti
- Prelievi e bonifici non autorizzati

Come difendersi

- Non dare mai codici al telefono
- Riagganciare e richiamare il numero ufficiale
- Prendersi tempo: l’urgenza è un trucco utilizzato dai truffatori

Cos’è il furto d’identità su WhatsApp

📊 Schema della truffa

- Il truffatore **ti scrive su WhatsApp usando l’account di un tuo contatto che è già stato vittima**.
- Il messaggio chiede il **codice di verifica a 6 cifre** che WhatsApp ti invia via SMS.
  (Ciao, ti ho inviato per sbaglio un codice di 6 cifre via sms, rimandamelo per favore)
- Se invii il codice, **il tuo account WhatsApp viene rubato**.
- L’account rubato viene poi usato per contattare altri → **effetto domino**.

📝 Descrizione

Messaggio falso che ti invita a inviare il codice di verifica ricevuto, sembra provenire da amici o da WhatsApp stesso e punta a creare **urgenza o pressione** per farti sbagliare.

Cos’è il furto d’identità su WhatsApp

⚠️ Rischio

- Perdita di accesso al tuo account WhatsApp.
- Possibile uso dell’account rubato per **truffare i tuoi contatti**.
- Diffusione di malware.
- Impatto sulla reputazione e perdita di privacy (messaggi falsi inviati a nome tuo).

🛡️ Come difendersi

- **Non condividere mai** il codice ricevuto via SMS.
- Ignora messaggi sospetti su WhatsApp, anche se provengono da amici.
- Se ti arriva un codice da un amico o parente con la richiesta di digitarlo è sicuro una truffa.

Truffe negli acquisti online

 Schema della truffa

- Offerte molto convenienti spesso su **social** o siti non ufficiali
- Venditore sconosciuto
- Pagamento anticipato

 Descrizione

Dopo il pagamento il prodotto non arriva oppure arriva molto in ritardo, oppure è diverso o di qualità inferiore. Spesso il venditore sparisce e non risponde più.

Truffe negli acquisti online

⚠ Rischio

- Perdita del denaro
- Difficoltà nel recupero

Come difendersi

- Usare solo siti conosciuti
- Diffidare di prezzi troppo bassi
- Pagare con metodi tracciabili (Carta di credito, PayPal, Pagamenti su siti ufficiali e conosciuti, Bonifico solo verso aziende reali e verificate).
- Mai Pagare con metodi non tracciabili (Ricariche PostePay, Carte regalo, Criptovalute, Bonifici a privati sconosciuti)

Romance scam (truffe sentimentali)

Schema della truffa

- Il truffatore finge un **interesse amoroso**
- costruisce una **relazione emotiva** (online, chat, social, app di incontri)
- crea fiducia, affetto, a volte dipendenza emotiva
- **solo dopo** chiede soldi, favori, ricariche, “emergenze”, ecc.

Descrizione

Il truffatore crea un legame emotivo attraverso i social network o app di messaggistica (**Facebook, Instagram, WhatsApp**), **solo dopo** chiede denaro, favori, ricariche, “emergenze”, ecc

Romance scam (truffe sentimentali)

⚠️ Rischio

- Gravi perdite economiche
- Forte impatto emotivo

 Come difendersi

- Attento alle storie tristi
- Spesso usano foto troppo perfette (false)
- Diffidare di chi chiede soldi e aiuti online
- Se hai dubbi blocca il numero o l’accesso
- Parlare sempre con familiari o amici fidati

Falsi investimenti e criptovalute

📊 Schema della truffa

- Promesse di guadagni sicuri
- Ti contatta una persona (app di incontri, social, chat)
- Ti dice che ha guadagnato grazie a investimenti o crypto ti mostra screenshot finti di profitti e ti invita a “provare con poco”.
- All’inizio sembra funzionare… 👉 poi chiedono altre somme e soldi spariscono, …e anche loro

📝 Descrizione

Qualcuno promette guadagni facili, ti fa investire su una piattaforma finta e poi sparisce con i soldi. Nessun investimento garantisce guadagni certi.

Falsi investimenti e criptovalute

⚠ Rischio

- Perdita totale del capitale investito

Come difendersi

- Diffidare dei guadagni facili
- Non investire mai su consiglio di sconosciuti
- Chiedere consiglio a un esperto vero, meglio se lo conosci bene
- Per investire usa solo banche o piattaforme ufficiali, conosciute e regolamentate

Truffa del finto parente

Schema della truffa

- Arriva un messaggio WhatsApp o SMS
- Il messaggio è breve e confidenziale, ad esempio:

“Ciao mamma/papà, ho cambiato numero, questo è quello nuovo puoi caricarlo”
“Ho perso il cellulare, sto usando un telefono temporaneo”
“Ho fatto un incidente ti spiego dopo”

Descrizione

Dopo aver ottenuto fiducia, il truffatore chiede **soldi, bonifici, ricariche o codici**, sostenendo un’emergenza improvvisa.
Il trucco è che spesso il cuore e la paura prendono il sopravvento. Anche persone attente ci cascano.

Truffa del finto parente

⚠️ Rischio

- Perdita di denaro
- Coinvolgimento emotivo forte

🛡️ Come difendersi

- Regola d’oro per questo tipo di truffa: 👉 Non inviare mai soldi senza aver parlato direttamente con il parente, di persona o almeno al numero vecchio.
- Non inviare codici via WhatsApp o denaro
- Bloccare e segnalare il contatto sospetto
  Se dicono “non mi puoi chiamare, ma è urgente” → truffa quasi certa
- Parlane subito con altri parenti

Furto d’identità *“Quando qualcuno usa i tuoi dati personali al tuo posto”*

📊 Schema della truffa

- Raccolta di dati personali (email, documenti, password)
- Uso dei dati al posto della vittima

📝 Descrizione

I truffatori usano informazioni rubate per aprire conti, fare acquisti o chiedere prestiti a nome della vittima.
“Esempio: aprono una carta di credito a tuo nome o fanno acquisti online”

Furto d’identità

⚠️ Rischio

- Debiti non riconosciuti
- Problemi legali e burocratici
- Se parte l’indagine, il nome che salta fuori è il tuo
- I dati rubati servono per creare debiti e contratti intestati alla vittima, anche senza usare i suoi soldi direttamente.

Come difendersi

- Proteggere documenti e dati personali
- Non inviare foto di documenti online
- Usare password diverse per ogni servizio

Malware e ransomware (virus informatici)

Malware significa letteralmente *software malevolo*. Questa categoria include **tutti i programmi creati per danneggiare o sfruttare** un computer, uno smartphone o una rete.

Come arriva (le vie più comuni)

- **Email** con allegati o link (finte fatture, corrieri, banche)
- **Siti web compromessi** o falsi
- **Download di app/programmi pirata**
- **Chiavette USB** sconosciute
- **Aggiornamenti finti** (“aggiorna Flash”, “aggiorna il browser”)

Cosa può fare un malware

- Spiare quello che fai (keylogger)
- Rubare password e dati bancari
- Usare il tuo dispositivo per altre truffe
- Installare **altri malware** (compreso il ransomware)

Malware e ransomware (virus informatici)

Il **ransomware** è una **sottocategoria** di malware, ed è tra le più pericolose.
👉 Il suo scopo è **bloccare i tuoi dati** e **chiedere un riscatto** (ransome=riscatto)
Infezione → Blocco file/dispositivo → Richiesta riscatto

Entra nel sistema (di solito via email o sito infetto)
Cripta file: documenti, foto, database
Ad esempio, può mostrare **un messaggio**:
“I tuoi file sono stati bloccati. Paga entro 72 ore”
Minaccia di:
cancellare i file
pubblicare i dati rubati
Le truffe e i virus informatici non colpiscono solo i singoli, ma anche grandi istituzioni.

Malware e ransomware (virus informatici)

⚠ Rischio

- Perdita di foto e documenti
- Blocco del dispositivo
- Senso di paura, ansia, panico

Come difendersi

- Non aprire allegati sospetti
- Tenere antivirus aggiornato
- Tenere il sistema operativo aggiornato
- Fare copie di sicurezza dei dati (backup)

Malware e ransomware (virus informatici)

- Malware : termine generico per tutti i programmi dannosi (virus, trojan, **ransomware**, spyware)
- Virus : tipo di malware che si replica e si diffonde (es. allegati email, chiavette USB)
- Avere un antivirus aggiornato protegge la maggior parte delle minacce comuni ma è utile ricordare che nessun antivirus garantisce sicurezza totale, quindi la prudenza e il backup rimangono fondamentali

Finta assistenza tecnica

📊 Schema della truffa

Mail, telefonata o Compare una schermata che dice : “Il suo computer è infetto, c*hiama subito l’assistenza Microsoft Non spegnere il PC*”

📝 Descrizione

Il truffatore si finge tecnico (Microsoft, Apple, Google) per prendere il controllo del computer.

Finta assistenza tecnica

⚠ Rischio

- Furto di dati
- Installazione di virus

Come difendersi

- Nessuna azienda chiama spontaneamente
- Non consentire MAI accesso remoto da pare di qualcuno
- Spegnere il computer e chiedere aiuto a una persona fidata

Tipo di truffa	Descrizione breve	Rischio principale	Difesa chiave
Phishing	Email o messaggi falsi che chiedono dati	Furto di password, denaro	Non cliccare link sospetti, prima verificare sempre
Smishing	SMS ingannevoli	Virus o furto dati	Non cliccare link, verificare con il servizio reale
Vishing	Telefonate da falsi operatori	Accesso ai conti, truffe	Non dare codici, richiamare il numero ufficiale
Furto d'identità su WhatsApp	Messaggio falso che ti invita a inviare il codice di verifica	Perdita di accesso al tuo account WhatsApp	Non condividere mai il codice ricevuto via SMS
Acquisti online falsi	Offerte troppo belle per essere vere	Perdita denaro	Usare siti affidabili, pagamenti tracciabili
Romance scam	Truffe sentimentali	Perdita denaro ed emotiva	Non inviare soldi, chiedere consiglio a familiari
Falsi investimenti	Promesse di guadagni certi	Perdita totale capitale	Diffidare guadagni facili, chiedere esperti
Truffa del finto parente	Messaggi da finti familiari	Perdita denaro	Verificare chiamando, non inviare soldi/codici
Furto d'identità	Uso dei dati rubati	Debiti e problemi legali	Proteggere dati, password diverse
Malware/Ransomware	Virus o file bloccati	Perdita dati o blocco device	Antivirus aggiornato, backup dati
Finta assistenza tecnica	Telefonate /msg di tecnici falsi	Furto dati, virus	Non consentire accesso remoto, spegnere e chiedere aiuto

Regole importanti

Le truffe funzionano perché **sfruttano emozioni e urgenza**, non la nostra intelligenza.

Regole d'oro:

- **Fermarsi e riflettere**
- **Non fornire dati personali o soldi a sconosciuti**
- **Verificare sempre le informazioni**
- **Chiedere aiuto a familiari o amici fidati**

Essere prudenti vuol dire «proteggersi» e non essere diffidenti.

Regole importanti di sicurezza digitale

Situazione	Cosa fare	Perché
Computer, cellulare, tablet	Impostare sempre un codice di sblocco (PIN, impronta, volto)	Così si evitano accessi se il dispositivo viene perso o rubato
Password	Usare password diverse per servizi diversi	Se una viene rubata, le altre restano sicure
Password sicura	Almeno 8–10 caratteri, lettere + numeri	Più difficile da indovinare
Dove conservarle	Su quaderno personale e sicuro senza scrivere «pssw», non tenerle nel telefono. O un gestore di password per chi ha dimestichezza con il computer	Metodo semplice e sicuro
Codici OTP	Non comunicarli a nessuno	Sono la chiave del conto
Aggiornamenti	Accettare aggiornamenti ufficiali di sistema	Correggono falle di sicurezza
Aiuto	Chiedere a un familiare o persona fidata	Meglio chiedere che rischiare

Regole importanti

“Criptare o Crittografare” significa **rendere i dati illeggibili a chi non ha la password**.
Se qualcuno ruba il tuo computer o l’hard disk, **non può leggere i file senza la tua password**.

2FA significa **Two-Factor Authentication**, in italiano: **autenticazione a due fattori**.
È un sistema di sicurezza che **richiede due “prove” per accedere a un account**, non solo la password. Quindi anche se qualcuno rubasse la tua password, **non può entrare senza il secondo fattore**.

💡 **Esempio concreto:**
Accedi al tuo account Google → inserisci la password → ricevi un codice sul telefono → inserisci il codice → accesso consentito.

Cosa sono i codici OTP

OTP significa *One Time Password* → **password valida una sola volta**.
È un **codice temporaneo** (di solito 6 cifre) che serve per:

- entrare in banca
- confermare un pagamento
- accedere a email o servizi importanti

Arriva tramite:

- **SMS**
- **app della banca**
- **app di autenticazione**

Cosa sono i codici OTP

👉 **Il codice OTP NON si dice MAI a nessuno.**
Nemmeno se dicono di essere la banca tramite un messaggio urgente o chiamano al telefono e sembra un tecnico

👨‍💼 **Come funziona una truffa con OTP**
Il truffatore:
1️⃣ ottiene la tua password (con email o SMS falsi)
2️⃣ prova ad entrare
3️⃣ **tu ricevi l'OTP vero**
4️⃣ lui ti chiama e dice:
"Ci serve il codice per bloccare l'accesso"
❌ Se glielo dai → **entra davvero lui**

Cosa sono i codici OTP

Se arriva un OTP **senza che tu stia facendo nulla**, è un allarme

✔ Non rispondere a chiamate o messaggi
✔ Chiudi tutto
✔ Chiama tu la banca (numero ufficiale)

“Il codice OTP è come la chiave di casa.
Se lo dai a qualcuno, entra lui.
La banca non lo chiede mai.”

Clonazione carte / bancomat:

È una truffa **reale**, soprattutto **anni fa**.

Come avveniva (e a volte avviene ancora)

- **Skimmer** installati su:
  - bancomat manomessi
  - vecchi POS poco sicuri
- Copiavano la **banda magnetica**
- Il PIN veniva:
  - spiato
  - ripreso con micro-telecamere

Clonazione carte / bancomat:

Le carte contactless **emettono pochissimi dati**
Non contengono il PIN
I limiti di spesa sono bassi
Servirebbe un lettore molto vicino
👉 **È teoricamente possibile**, ma **nella pratica è più raro**

Molto più facile essere truffati:
online
via phishing
con finti operatori (vishing)
Oggi i rischi principali sono **online e al telefono**

Clonazione carte / bancomat:

PIN e sicurezza

Senza PIN **non si fanno grosse spese**

Le banche oggi di solito:

- bloccano operazioni sospette
- avvisano subito
- rimborsano spesso (se segnalato e denunciato subito)

Per spese via Internet usare anche una carta prepagata, meno rischioso poiché contiene un importo limitato

Nuove Frontiere basate sull'IA

Voice Cloning (Vishing 2.0): I truffatori clonano la voce di un tuo familiare o del tuo capo per richiedere trasferimenti di denaro urgenti durante una telefonata.
Deepfake Video: Utilizzo di volti noti o dirigenti d'azienda in videochiamate per autorizzare pagamenti fraudolenti.
Phishing Perfetto: Messaggi ed email scritti senza errori grammaticali, generati da IA, che imitano perfettamente lo stile di banche o enti pubblici.

FINE DELLA PRESENTAZIONE