GUIDA COMPLETA ALLA PROTEZIONE DAL PHISHING

Una guida pratica per riconoscere e difendersi dalle truffe online

INDICE

a) CHE COS'È IL PHISHING?

Il **phishing** è una truffa online dove i criminali si fingono aziende o organizzazioni legittime (come banche, Poste Italiane, Amazon, etc.) per rubare le vostre informazioni personali.

Cosa Cercano i Truffatori:

Password dei vostri account

Numeri di carte di credito o bancomat

Codici fiscali e documenti di identità

Codici di accesso all'home banking

PIN e codici di sicurezza

Come Funziona:

1) Vi inviano un'e-mail **falsa** che sembra vera
2) Vi chiedono di cliccare su un **link pericoloso**
3) Vi portano su un **sito web falso** (ma che sembra quello vero)
4) Vi chiedono di **inserire i vostri dati personali**
5) **Rubano le vostre informazioni** per svuotare conti o fare acquisti

b) **COME RICONOSCERE UN TENTATIVO DI PHISHING**

CONTROLLATE SEMPRE IL MITTENTE

❌ **SEGNALI DI PERICOLO:**

- E-mail da indirizzi strani: banc4@gmail.com invece di info@unicredit.it
- Nomi scritti male: "Amazom" invece di "Amazon"
- Domini sospetti: .tk, .ml, .ga invece di .it o .com

✅ **COSA VERIFICARE:**

- L'indirizzo e-mail deve corrispondere esattamente a quello ufficiale
- Se avete dubbi, andate direttamente sul sito ufficiale dell'azienda
- Chiamate il numero verde ufficiale per verificare

ATTENZIONE AL CONTENUTO

❌ **FRASI TIPICHE DEI TRUFFATORI:**

- "Il suo account verrà chiuso entro 24 ore"
- "Confermi immediatamente i suoi dati"
- "Ha vinto un premio, clicchi qui"
- "Sospesa attività sospetta sul suo conto"
- "Aggiornamento urgente richiesto"

✅ **RICORDATE:**

- Le banche NON chiedono mai password via e-mail
- I concorsi veri non richiedono soldi per ritirare premi
- Le aziende serie danno sempre tempo per rispondere

c) **I SEGNALI DI ALLARME DA NON IGNORARE**

🚨 **URGENZA FALSA**

- "IMMEDIATO", "URGENTE", "ENTRO OGGI"
- Minacce di chiusura account
- Richieste di azione immediata

🚨 ERRORI NEL TESTO

- Errori di grammatica o ortografia
- Caratteri strani o simboli insoliti
- Traduzioni approssimative dall'inglese

🚨 RICHIESTE SOSPETTE

- Chiedono password complete
- Vogliono PIN o codici segreti
- Richiedono documenti per e-mail

🚨 LINK PERICOLOSI

- URL abbreviati (bit.ly, tinyurl.com)
- Indirizzi che non corrispondono all'azienda
- Link che iniziano con numeri invece che lettere

d) TIPI COMUNI DI PHISHING

📧 EMAIL PHISHING

Esempio tipico: "Gentile Cliente, il suo account Poste Italiane è stato sospeso per attività sospette. Clicchi qui per riattivarlo entro 24 ore."

Come riconoscerlo:

- Non usano il vostro nome
- Urgenza eccessiva
- Link sospetti

📱 SMS PHISHING (SMISHING)

Esempio tipico: "La sua carta è stata bloccata. Clicchi: www.sito-falso.com per sbloccarla"

Come riconoscerlo:

- SMS da numeri strani
- Link corti e sospetti
- Richieste immediate

📞 PHONE PHISHING (VISHING)

Esempio tipico: "Sono della sua banca, c'è un problema con il conto. Mi dia il codice che le arriva per SMS"

Come riconoscerlo:

- Chiamate non richieste
- Chiedono codici al telefono
- Pressione per agire subito

🎣 PHISHING SUI SOCIAL

Esempio tipico: Post su Facebook: "Clicca qui per vedere chi visita il tuo profilo!"

Come riconoscerlo:

- Promesse irrealistiche
- Link esterni sospetti
- Richieste di dati personali

e) **COME PROTEGGERSI: REGOLE D'ORO**

🛡️ **REGOLA N°1: MAI CLICCARE LINK SOSPETTI**

- Se avete dubbi, NON cliccate
- Andate direttamente sul sito ufficiale
- Digitate l'indirizzo nella barra del browser

🛡️ **REGOLA N°2: VERIFICATE SEMPRE**

- Chiamate il numero verde ufficiale
- Chiedete conferma in filiale
- Controllate gli estratti conto regolarmente

🛡️ **REGOLA N°3: NON DATE MAI DATI SENSIBILI**

- **MAI password complete via email**
- **MAI PIN o codici segreti al telefono**
- **MAI dati della carta a sconosciuti**

🛡️ **REGOLA N°4: MANTENETE AGGIORNATI I DISPOSITIVI**

- Installate gli aggiornamenti di sicurezza
- Usate un antivirus aggiornato
- Attivate il firewall

🛡️ **REGOLA N°5: USATE PASSWORD SICURE**

- Diverse per ogni account importante
- Almeno 8 caratteri con numeri e simboli
- Cambiatele se sospettate problemi

f) **COSA FARE SE SIETE VITTIME DI PHISHING**

🚨 **AZIONI IMMEDIATE (ENTRO 1 ORA)**

1. CAMBIATE SUBITO LE PASSWORD

- Account e-mail
- Home banking
- Tutti gli account importanti

2. CONTATTATE LA BANCA

- Chiamate immediatamente il numero verde
- Fate bloccare carte e conti se necessario
- Richiedete un nuovo PIN

3. CONTROLLATE I MOVIMENTI

- Verificate estratti conto
- Controllate movimenti recenti
- Segnalate transazioni sospette

📋 **AZIONI DA FARE ENTRO 24 ORE**

4. DENUNCIATE ALLE AUTORITÀ

- Polizia Postale: www.commissariatodips.it
- Carabinieri: 112
- Conservate tutte le prove (e-mail, SMS, screenshot)

5. INFORMATE ALTRI

- Avvertite familiari e amici
- Segnalate la truffa sui social
- Aiutate a prevenire altre vittime

g) **IMPOSTAZIONI DI SICUREZZA CONSIGLIATE**

📧 **CONFIGURAZIONE EMAIL**

Gmail:

1) Andate in Impostazioni
2) Attivate "Filtro antispam avanzato"
3) Attivate la "Verifica in due passaggi"

Outlook/Hotmail:

1) Impostazioni → Sicurezza
2) Attivate "Protezione avanzata"
3) Configurate l'autenticazione a due fattori

🔐 SICUREZZA DELL'HOME BANKING

Impostazioni consigliate:

- Attivate SMS di notifica per ogni operazione
- Impostate limiti di spesa giornalieri bassi
- Attivate il blocco automatico dopo tentativi falliti
- Non salvate mai le password nel browser

📱 SICUREZZA SMARTPHONE

iPhone:

- Attivate "Blocco automatico" dopo 5 minuti
- Usate Touch ID o Face ID
- Aggiornate iOS regolarmente

Android:

- Attivate "Verifica app dannose"
- Installate app solo da Google Play Store
- Mantenete aggiornato il sistema

h) ESEMPI PRATICI DI EMAIL FRAUDOLENTE

🚫 ESEMPIO 1: FINTA BANCA

OGGETTO: "URGENTE: Sospensione account UniCredit"

TESTO: "Gentile Cliente, Il suo account è stato temporaneamente sospeso per attività sospetta. Per riattivarlo clicchi qui: www.unicredit-sicurezza.tk Grazie, Staff UniCredit"

SEGNALI DI PERICOLO:

1) Dominio falso (.tk invece di .unicredit.it)
2) Non usa il vostro nome
3) Urgenza eccessiva
4) Grammatica imperfetta

🚫 ESEMPIO 2: FINTO AMAZON

OGGETTO: "Il suo ordine è stato annullato"

TESTO: "Caro cliente, Il suo ultimo ordine di €299 è stato annullato per problemi di pagamento. Clicchi qui per aggiornare la carta: bit.ly/amazon-pay, Cordiali saluti"

SEGNALI DI PERICOLO:

1) Link abbreviato sospetto
2) Non specifica quale ordine
3) Richiesta di aggiornare dati di pagamento

🚫 ESEMPIO 3: FINTE POSTE ITALIANE

OGGETTO: "Pacchi in giacenza - Azione richiesta"

TESTO: "Abbiamo un pacco per lei che non siamo riusciti a consegnare. Paghi la giacenza di €2.50 qui:www.poste-italiane.org Pacco restituito al mittente tra 48 ore."

SEGNALI DI PERICOLO:

1) Dominio falso (.org invece di .poste.it)
2) Richiesta di pagamento online
3) Urgenza per creare pressione

i) CHECKLIST DI SICUREZZA GIORNALIERA

✅ PRIMA DI APRIRE UN'EMAIL:

- Riconosco il mittente?
- L'indirizzo e-mail è corretto?
- Il messaggio sembra autentico?
- Ci sono errori grammaticali evidenti?
- Mi viene chiesto di agire con urgenza?

✅ **PRIMA DI CLICCARE UN LINK:**

- ☐ Il link porta al sito ufficiale?
- ☐ Posso verificare l'informazione altrimenti?
- ☐ Ho davvero bisogno di cliccare ora?
- ☐ Posso digitare l'indirizzo direttamente?

✅ **PRIMA DI INSERIRE DATI PERSONALI:**

- ☐ Sono sicuro che il sito sia autentico?
- ☐ C'è il lucchetto di sicurezza (https)?
- ☐ L'azienda mi ha davvero chiesto questi dati?
- ☐ Posso fornire queste informazioni per telefono invece?

✅ **CONTROLLI SETTIMANALI:**

- ☐ Ho controllato i movimenti bancari?
- ☐ Le mie password sono ancora sicure?
- ☐ Ho aggiornato antivirus e sistema operativo?
- ☐ Ho verificato le attività sui miei account social?

j) CONTATTI UTILI

🚓 FORZE DELL'ORDINE

Polizia Postale

- **Sito web:** www.commissariatodips.it
- **Email:** poltel@interno.it

Carabinieri

- **Numero emergenza:** 112

🏦 NUMERI VERDI BANCHE PRINCIPALI

Intesa Sanpaolo: 800-303.303

UniCredit: 800-57.57.57

Banco BPM: 800-024.024

Monte dei Paschi:800-41.41.41

ING Direct: 800-71.72.73

📮 SERVIZI POSTALI

Poste Italiane: 803.160

PostePay: 800.00.33.22

🛒 SERVIZI ONLINE

Amazon: 800-145.851

PayPal: 06 8938 6461

🆘 ASSISTENZA TECNICA

TIM: 187

Vodafone: 190

Fastweb: 192.193

WindTre: 159

Iliad: 177

CONCLUSIONI

Ricordate sempre:

1) **La fretta è nemica della sicurezza** - Prendetevi sempre tempo per verificare
2) **Le aziende serie non chiedono mai dati sensibili via email**
3) **In caso di dubbio, chiamate sempre il numero ufficiale**
4) **È meglio essere prudenti che dispiaciuti**
5) **Condividete queste informazioni con familiari e amici**

📞 IN CASO DI DUBBI

Se ricevete e-mail, SMS o chiamate sospette e non sapete come comportarvi:

1) **NON** cliccate nulla
2) **NON** fornite informazioni
3) **Chiedete aiuto** a un familiare o amico esperto
4) **Chiamate** direttamente l'azienda interessata
5) **Segnalate** il tentativo di truffa alle autorità

La vostra sicurezza online è importante. Con un po' di attenzione e queste semplici regole, potrete navigare e utilizzare i servizi digitali in tranquillità.

Questa guida è stata preparata per aiutarvi a riconoscere e difendervi dalle truffe online. Conservatela e consultatela ogni volta che avete dubbi su e-mail, messaggi o chiamate sospette.

Giovanni Di Marco

Consulente Informatico ed Esperto di Sicurezza Digitale
Titolare di **Intes Informatica San Mauro Pascoli (FC)**

Con oltre 20 anni di esperienza nel settore IT, aiuto quotidianamente aziende e privati a proteggersi dalle minacce informatiche. Ho creato questa guida per condividere gratuitamente le conoscenze necessarie a difendersi dal phishing.

Contatti:

📧 info@intesinformatica.it
📱 +39 393 789 799
🌐 www.intesinformatica.it

Versione: 1.0 - Luglio 2025 **Prossimo aggiornamento:** gennaio 2026