SICUREZZA

Obiettivo del modulo

Imparare a riconoscere i rischi legati all'uso di internet e dei programmi digitali in ufficio, per proteggere i dati personali e quelli aziendali da truffe, virus e furti di informazioni.

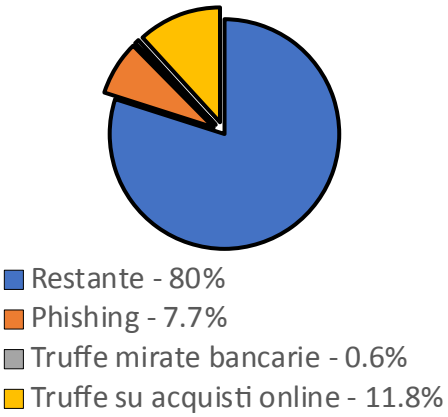
---

1. Perché la sicurezza è importante

Dove ci sono **soldi** e **dati personali**, c'è sempre un rischio. Ogni giorno si registrano nuovi tentativi di truffa online e attacchi informatici. Le statistiche mostrano che questi fenomeni sono in aumento.

- **7,7%** casi di phishing
- **11%** truffe online
- **0,6%** truffe bancarie

Fonte: ISTAT 2015–2016 (link)



Anche se i dati sono vecchi, oggi la digitalizzazione è aumentata molto, quindi anche le truffe sono cresciute. Inoltre, molte persone non denunciano per vergogna o paura, quindi i numeri reali sono probabilmente più alti.

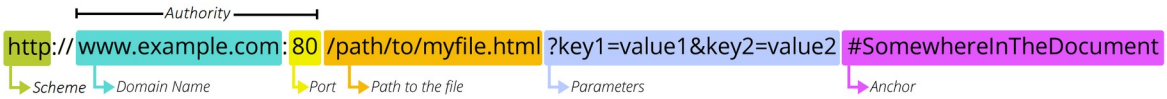
Significato dei termini

- **Phishing:** truffa che cerca di ottenere i tuoi dati (es. login o carta di credito) fingendo di essere una fonte affidabile.
- **Malware:** software dannoso che può infettare il tuo computer.
- **Truffa online:** qualunque tentativo di frode tramite internet (email, social, annunci falsi, ecc.).

---

2. Riconoscere un dominio sicuro

Quando navighiamo su internet, la **barra degli indirizzi** mostra il nome del sito, chiamato **dominio**. È fondamentale saperlo leggere per non cadere in trappole.



Come riconoscerlo

- La parte **più importante** è quella che viene prima del ".com", ".it", ".org", ecc.
  - Esempio: in `https://www.google.com/maps`, il dominio è **google.com**.
- Un sito falso può usare indirizzi simili, come `google-login.com` o `g00gle.com`.

- L’ordine è anche importante, la parte più a destra è più importante e ha la priorità, nello specifico trovare `google.login.com` è diverso da `login.google.com.` Il primo è di proprietà di login.com, il secondo di google.com

Nei principali browser

- **Google Chrome:** mostra in **grassetto** la parte principale del dominio.
- **Safari:** mostra solo la parte essenziale, rendendo più chiaro quale sia il sito reale.

Se l’indirizzo ti sembra strano, **non inserire mai dati personali o bancari.**

---

3. Pratiche di sicurezza sui file

Quando scarichi o apri un file, **controlla sempre il tipo di estensione** (cioè le ultime lettere dopo il punto nel nome del file).

Dove vedere il tipo di file

- Su **Windows**, apri una cartella e vai su **Visualizza → Estensioni nomi file** per attivarle.
- Su **Mac**, premi ⌘ + I (Ottieni informazioni) e guarda la voce *Tipo*.

Estensioni pericolose

Alcuni tipi di file possono eseguire programmi e infettare il PC.

File vettori di possibile malware diretti

`.exe` `.scr` `.vbs` `.js` `.bat` `.ps` `.msi` `.jar` `.hta` `.dll`

Evita sempre di aprirli, soprattutto se arrivano da email o link sconosciuti.

File vettori di malware con interazione

`.docx` `.xls` `.ppt`

Questi sembrano documenti normali, ma possono contenere **macro** (piccoli programmi) pericolose.

Minacce più avanzate

- **File ZIP protetti da password:** spesso usati per nascondere virus all’interno.

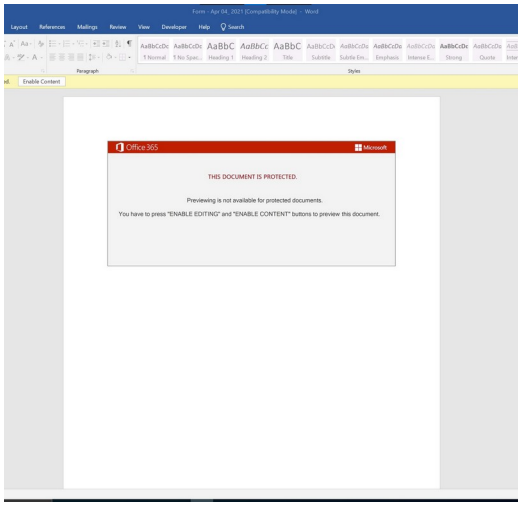
Se un file ti chiede di “abilitare contenuto” o “eseguire script”, sospendi subito l’azione e chiedi conferma a un tecnico o al tuo responsabile.

---

4. I Malware nei documenti Office

Quando apri un documento Office (Word, Excel, PowerPoint), può comparire un messaggio come:

> “Questo documento è protetto. Clicca su ‘Abilita modifica’ per visualizzare il contenuto.”



Se non conosci la provenienza del file, **non abilitarla mai**.
Quella funzione serve per attivare macro, ma i truffatori la usano per installare virus.

Regole pratiche

1. Apri documenti solo da fonti conosciute.
2. Se ti viene chiesto di abilitare modifiche o script, **rifiuta**.
3. In caso di dubbio, chiudi il file e contatta l’autore per verificare.

---

5. Le email: il principale vettore di truffe

La **posta elettronica** è il mezzo più usato per diffondere virus o tentativi di frode. Spesso i truffatori cercano di farti cliccare su link o aprire allegati.

Regole generali per riconoscere una mail sospetta

- **Non aprire link** contenuti in email sospette.
- **Non inserire mai** dati bancari o di carte di credito dopo aver cliccato su un link.
- **Non aprire allegati** non attesi, anche se il mittente sembra conosciuto.
- **Non fidarti** delle email che fingono di provenire da banche o enti pubblici e ti avvisano di “problemi sul conto”.
- **Dubbi?** Chiama direttamente la banca o l’ente usando i contatti ufficiali (mai quelli nell’email stessa).

Segnali di allarme

- Errori grammaticali o grafici nel testo.
- Mittente con indirizzo insolito (es. assistenza@bancha.it invece di banca.it).
- Pressione o urgenza (es. “Il tuo conto sarà bloccato!”).

Esempio pratico

Un’email ti dice: “Aggiorna subito i tuoi dati cliccando qui”.

- **Non cliccare.** Vai tu sul sito ufficiale digitando l’indirizzo manualmente nel browser.

---

6. Virus (Ransomware)

Il **ransomware** è un tipo di malware che **cifra i dati dell'utente**, rendendoli inaccessibili, e **chiede un riscatto** per ripristinarli.
Può paralizzare completamente le operazioni aziendali.
Come proteggersi:

- Usare sempre software antivirus aggiornati.
- Effettuare **backup regolari** dei dati.
- Formare il personale sulla **sicurezza informatica** e sulle buone pratiche (non aprire allegati sospetti, aggiornare i programmi, ecc.).

7. Furti di dati (Data Breach)

I **furti di dati** si verificano quando informazioni sensibili vengono **rubate senza autorizzazione**.
Possono derivare da vulnerabilità del sistema, o da furti di dati nelle piattaforme nelle quali siamo iscritti.

Come prevenirli:

- Attivare l'**autenticazione multifattoriale (MFA)** per gli accessi.
- Mantenere una **sorveglianza continua** delle attività informatiche.
- Utilizzare **password diverse** per ogni servizio interniet

I furti di dati avvengono **giornalmente**, tanto che sono disponibili delle liste **pubbliche** con oltre 15,000,000,000+ dati rubati.

Possiamo verificare se la nostra mail si trova nelle liste pubbliche su https://haveibeenpwned.com/ .

Strategie della password:

- Almeno **8 caratteri**
- Una lettera **maiuscola** e una **minuscola**
- Un **numero**
- Un **simbolo**

Suggerimento password mnemoniche:

Le password mnemoniche sono password complesse ma facili da scrivere. Si generano scegliendo **3 numeri** casuali e **3 parole** a casuali dal dizionario italiano. Queste poi le possiamo **combinare** per formare una password del tipo `Pizza3-Albero6-Cinghia2`

8. Furti d’identità

Il **furto d’identità** avviene quando dati personali come nome, codice fiscale o dati bancari vengono **usati illegalmente** per frodi.
Le vittime possono subire danni economici e legali.

Come prevenirlo:

- Proteggere le proprie informazioni personali.
- Riconoscere e segnalare email o messaggi sospetti (**phishing**, **scam**).
- Utilizzare strumenti di sicurezza avanzati per autenticazione e navigazione.

Crimine informatico e abuso degli strumenti digitali
In un mondo sempre più connesso, i criminali usano la tecnologia per **commettere reati** come:

- Violazione di sistemi informatici.
- Diffusione di malware.
- Furto di dati sensibili.

L’abuso di strumenti digitali può avere **effetti devastanti** su individui, aziende e istituzioni.
È importante mantenere aggiornati i software e seguire politiche di sicurezza adeguate.