Formation Prevention

GUIDA AI BUONI RIFLESSI

# Prevenire le trappole di tutti i giorni

12 temi, i gesti che proteggono la Sua azienda. Da tenere a portata di mano.



formation-prevention.ch

PRIMA DI INIZIARE

# Tre riflessi validi ovunque

**1** **Si fermi un attimo**

L'urgenza, la paura o una ricompensa troppo bella sono le leve preferite dei truffatori. Una richiesta pressante è proprio il momento di rallentare.

**2** **Verifichi tramite un altro canale**

Richiami la persona o l'azienda al numero che conosce già, mai a quello indicato nel messaggio.

**3** **Segnali subito**

Al servizio informatico o al Suo responsabile, anche in caso di semplice dubbio, e anche se ha già cliccato.

Questa guida riassume i 12 moduli di Formation Prevention. Non sostituisce i moduli: glieli ricorda, tema per tema.

TEMA 01 / 12

# Phishing

> Un'e-mail, un SMS o un codice QR trappola cura tutto ciò che Lei vede: il nome del mittente, il logo, il tono. Ciò che lo tradisce è nascosto.

### Guardi l'indirizzo reale

Il nome visualizzato si sceglie liberamente. Legga l'indirizzo completo del mittente e passi il mouse su un link (pressione lunga sul telefono) per vedere dove porta davvero.

### Diffidi dell'urgenza

Pacco trattenuto, conto bloccato, fattura non pagata: una scadenza molto breve è un segnale d'allarme, non un motivo per agire in fretta.

### Digiti Lei l'indirizzo

Per accedere alla Sua banca o a un servizio, inserisca l'indirizzo che conosce invece di seguire il link ricevuto.

### Codici QR

Non scansioni un codice QR incollato su un parchimetro o ricevuto per posta senza verificare l'indirizzo che apre.

DA RICORDARE

Messaggio sospetto: non clicchi, non risponda, non lo inoltri a un collega. Lo segnali al servizio informatico o a reports@antiphishing.ch.

TEMA 02 / 12

# Usurpazione d'identità

> Un falso direttore, fornitore o fiduciario chiede un bonifico urgente e confidenziale, o una modifica delle coordinate bancarie.

- **Richiami al numero conosciuto**

  Contatti la persona tramite un numero che aveva già, mai quello indicato nel messaggio o nella chiamata.

- **Rispetti la procedura**

  Un pagamento insolito passa dal doppio controllo previsto, anche se il «direttore» esige il segreto.

- **Modifica dell'IBAN**

  Ogni richiesta di modificare le coordinate bancarie di un fornitore va verificata per telefono prima di essere registrata.

- **Legga il dominio**

  Una sola lettera diversa nell'indirizzo del mittente basta al truffatore.

DA RICORDARE

Urgenza, segreto e pagamento insieme: si fermi e verifichi. Nessuno Le rimprovererà di aver verificato.

TEMA 03 / 12

# Password

> Una password corta o riutilizzata cade in fretta, e apre allora tutti gli account che la usano.

- **Prima la lunghezza**

  Almeno 12 caratteri, meglio 16 o più. Una frase facile da ricordare vale più di una parola complicata.

- **Una password per account**

  Se un sito si fa rubare i dati, i Suoi altri account restano protetti.

- **Un gestore di password**

  Crea e ricorda per Lei password solide: quello fornito dalla Sua azienda, o per esempio Bitwarden o Proton Pass.

- **Niente di personale**

  Né nome, né data di nascita, né nome dell'azienda, né anno: sono i primi tentativi di un pirata.

DA RICORDARE

Una sola password da ricordare davvero: quella del gestore. La renda lunga e unica.

TEMA 04 / 12

# Autenticazione a due fattori

> Con un secondo fattore, una password rubata non basta più per entrare nel Suo account.

- **La attivi ovunque**

  E-mail, gestore di password, account di lavoro: ovunque sia proposta.

- **Preferisca un'app**

  Un'app di autenticazione o una chiave di sicurezza protegge meglio di un codice ricevuto via SMS.

- **Non dia mai un codice**

  Né il servizio informatico né una banca glielo chiederanno, per telefono o per messaggio.

- **Rifiuti ciò che non ha richiesto**

  Richieste di accesso ripetute significano che qualcuno ha la Sua password: rifiuti, la cambi e avvisi il servizio informatico.

DA RICORDARE

Conservi i Suoi codici di recupero nel gestore di password, non in un'e-mail.

TEMA 05 / 12

# Navigazione web

> Un sito falso può essere identico a quello vero, lucchetto compreso.

- **Il lucchetto non basta**

  Cifra la connessione, ma non dice nulla dell'onestà del sito. Legga l'indirizzo completo.

- **Attenzione agli annunci**

  Nei risultati di ricerca, i link sponsorizzati possono essere pagati da truffatori: digiti piuttosto l'indirizzo ufficiale.

- **Download ufficiali**

  Installi un programma solo dal sito del suo editore, oppure chieda al servizio informatico.

- **Falsi allarmi**

  Un avviso di virus con conto alla rovescia o un numero da chiamare è una trappola: chiuda la scheda. Un avviso di certificato non va mai ignorato.

DA RICORDARE

In caso di dubbio su una pagina, la chiuda e passi dall'indirizzo che conosce.

TEMA 06 / 12

# Wi-Fi pubblico

> Al bar, in stazione o in albergo, qualcuno può spacciarsi per la rete ufficiale e vedere ciò che Lei invia.

- **Prima il Suo telefono**
  L'hotspot del Suo telefono è più sicuro di una rete aperta.
- **La VPN dell'azienda**
  La attivi prima di lavorare su una rete che non controlla.
- **Niente operazioni sensibili**
  Eviti l'e-banking e i dati confidenziali su una rete pubblica.
- **Pagine di accesso trappola**
  Una pagina che chiede una carta bancaria o l'installazione di un programma per accedere al Wi-Fi: rifiuti. Dimentichi la rete dopo l'uso.

DA RICORDARE

Una password esposta al bancone non trasforma una rete condivisa in una rete privata.

TEMA 07 / 12

# Ransomware

> Un ransomware cifra i file dell'azienda ed esige un riscatto. Entra spesso tramite un allegato trappola.

- **Non attivi il contenuto**

  Un documento ricevuto per e-mail che chiede di «attivare il contenuto» per essere visualizzato è un segnale d'allarme.

- **Schermo bloccato o file rinominati**

  Interrompa subito la connessione di rete (cavo e Wi-Fi), poi avvisi il servizio informatico e il Suo responsabile.

- **Non paghi**

  E non contatti i pirati: pagare non garantisce né il recupero dei file né che i dati non vengano pubblicati.

- **Non colleghi il backup**

  Il disco di backup verrebbe cifrato a sua volta. Lasci decidere il servizio informatico sul seguito.

DA RICORDARE

Interrompere la rete, poi dare l'allarme: due gesti, in quest'ordine.

TEMA 08 / 12

# Chiavette USB e supporti

> Una chiavetta trovata o regalata può contenere un programma malevolo, o persino fingersi una tastiera che digita comandi.

- **Mai una chiavetta sconosciuta**

  Una chiavetta trovata, ricevuta per posta o regalata a una fiera non si collega: la consegni al servizio informatico.

- **Chiavette cifrate**

  Per i dati di lavoro, usi i supporti cifrati forniti dall'azienda, non una chiavetta personale.

- **Eliminare non è cancellare**

  Eliminare dei file o formattare rapidamente non li cancella davvero: consegni i supporti usati al servizio informatico.

- **Supporto perso**

  Una chiavetta o un disco perso con dati dell'azienda si segnala subito.

DA RICORDARE

Ha collegato un supporto dubbio: lo scolleghi, interrompa la rete e avvisi.

TEMA 09 / 12

# Telelavoro

> A casa, il router Internet e il computer di lavoro sono la Sua prima protezione.

- **Configuri il router**

  Cambi la password di amministrazione originale, scelga WPA3 (almeno WPA2) e una password Wi-Fi di almeno 16 caratteri, idealmente 20.

- **Una rete ospiti**

  Per i visitatori e gli oggetti connessi, separata dal Suo computer di lavoro.

- **Un computer per il lavoro**

  Usato solo per lavoro, aggiornato e bloccato appena si alza. Accesso ai dati tramite la VPN dell'azienda.

- **Discrezione**

  Chiamate confidenziali e schermo al riparo da sguardi altrui, documenti riposti.

DA RICORDARE

Computer perso o rubato: avvisi immediatamente il servizio informatico.

TEMA 10 / 12

# Deepfake e vishing

> Una voce può essere imitata a partire da pochi secondi di registrazione, un volto in videoconferenza anche, e il numero visualizzato può essere falsificato.

- **Riattacchi e richiami**

  Al numero che conosce, anche se la voce è quella del Suo direttore.

- **Mai un codice al telefono**

  Nessuna password, nessun codice ricevuto via SMS, nessun PIN, chiunque chiami.

- **Nessun controllo a distanza**

  Rifiuti di installare un programma o di lasciare che uno sconosciuto (falso supporto, falsa polizia) controlli il Suo computer.

- **Il comportamento conta più dell'aspetto**

  Richiesta insolita, pressione, segreto: sono questi i segnali da ascoltare.

DA RICORDARE

Un dubbio durante una chiamata: metta fine alla conversazione. Il vero interlocutore capirà.

TEMA 11 / 12

# Backup e file sensibili

> Guasto, incendio, ransomware: senza un backup aggiornato e al sicuro, il lavoro è perso.

- **La regola 3-2-1**

  Tre copie dei dati, su due supporti diversi, di cui una in un altro luogo (raccomandazione dell'UFCS).

- **Una copia offline**

  Scolleghi il disco dopo ogni backup e verifichi regolarmente il ripristino.

- **Condividere con misura**

  Un file sensibile si condivide solo con le persone interessate, mai tramite un link aperto a tutti.

- **Destinatario sbagliato**

  Un documento inviato alla persona sbagliata si segnala subito: l'azienda può avere obblighi legali.

DA RICORDARE

Un backup mai ripristinato è solo una speranza.

TEMA 12 / 12

# Segnalazione di un incidente

> Ogni minuto conta: prima l'azienda viene avvisata, prima l'attacco viene fermato.

- **Subito**

  Segnali appena ha un dubbio, anche per un incidente evitato per un soffio.

- **Per telefono, se possibile**

  La Sua casella e-mail potrebbe essere già in mani sbagliate.

- **Dica l'essenziale**

  L'ora, cosa è successo, l'account o il messaggio interessato e cosa ha già fatto.

- **Non elimini nulla**

  E non minimizzi: sono indizi preziosi per il servizio informatico.

DA RICORDARE

Segnalare in fretta non è mai un errore.

IN CASO DI INCIDENTE

# I cinque gesti

1. **Si fermi**
   Non clicchi più. File cifrati: scolleghi la rete.
2. **Avverta subito, per telefono**
   Il servizio informatico e il Suo responsabile.
3. **Descriva con precisione**
   Cosa, quando, quale account o messaggio.
4. **Non cancelli nulla**
   Conservi le prove, non contatti gli attaccanti.
5. **Segua le istruzioni**
   Il servizio informatico sa cosa fare.

I SUOI CONTATTI

Servizio informatico _____

Responsabile _____

Numero d'emergenza _____

IN SVIZZERA

Segnalare un phishing
**reports@antiphishing.ch**

Ufficio federale della cibersicurezza (UFCS)
**www.bacs.admin.ch**

Danno finanziario
**La Sua polizia cantonale**

Formation Prevention

FORMATION PREVENTION

# Imparare vivendolo

Moduli di circa 10 minuti, simulazioni realistiche ed esempi svizzeri, perché i buoni riflessi diventino abitudini.

formation-prevention.ch

IMPRESSUM

Datalys
Grand Rue 8
1196 Gland
Svizzera

© 2026 Datalys