Modo Refugio

THE PLAYBOOK

Attacco informatico

I tuoi file in ostaggio

Versione online aggiornata

08:31 · LA TUA SCRIVANIA 08:31. Apri il portatile e lo sfondo non è più il tuo. Scritte rosse. Un conto alla rovescia: 71:59:43. «I tuoi file sono stati cifrati». Ti torna in mente l'email di ieri, quella che sembrava della banca. Il telefono vibra: un SMS chiede di «confermare un codice». Un altro. Un altro ancora. Il mouse si muove ancora. Le tue foto hanno estensioni che non riconosci. **L'istinto ti dice di pagare. Non toccare niente prima di aver letto qui.**

Prima di tutto

1. **Scollega** da internet il dispositivo colpito (wifi e cavo). Non spegnerlo se c'è un ransomware.
2. **Non pagare** nessun riscatto e non seguire le istruzioni degli attaccanti.
3. Chiama la tua **banca** se qualcuno può aver avuto accesso a conti o carte.
4. Segnala alla **Polizia Postale** (Commissariato di PS Online) e conserva le prove.

1 Se l'attacco è contro di te

PRIMI 30 MINUTI

- [ ] **Isola il dispositivo: stacca wifi e cavo di rete. Non collegare chiavette USB né dischi di backup a quel computer.**
- [ ] **Da un altro dispositivo pulito, cambia prima la password dell'email (è la chiave di tutto) e poi quelle di banca e social. Attiva l'autenticazione a due fattori.**
- [ ] Chiama la banca al numero ufficiale (quello sulla carta o sul sito, mai quello di un SMS) per bloccare le carte e controllare i movimenti.
- [ ] Fai screenshot di messaggi, email e addebiti: sono prove.
- [ ] Avvisa i tuoi contatti se qualcuno si è spacciato per te su WhatsApp o sui social.

2 Le ore successive

IN GIORNATA

- [ ] Fai una segnalazione sul portale del Commissariato di PS Online della Polizia Postale e, se ci sono perdite economiche, sporgi denuncia.
- [ ] Disconosci le operazioni non autorizzate con la banca il prima possibile: i tempi contano per il rimborso.
- [ ] Ripristina i file solo da backup che non erano collegati durante l'attacco.
- [ ] Controlla sessioni aperte e dispositivi collegati nei tuoi account principali e chiudili.

3 Se l'attacco è di massa

SERVIZI GIÙ

- [ ] Tieni contanti per qualche giorno: carte, app di pagamento e bancomat possono non funzionare.
- [ ] **Diffida di qualsiasi SMS, chiamata o email che «ti aiuta» con il problema: i truffatori approfittano delle crisi.**

- [ ] Informati solo da canali ufficiali (ACN, la tua banca, il Governo) e media riconosciuti.
- [ ] Se hai visite mediche o pratiche, chiama o vai di persona prima di darle per perse.

NON fare

- ✕ Pagare riscatti: non garantisce di recuperare nulla e finanzia nuovi attacchi.
- ✕ Cliccare link in SMS o email che dicono di arrivare dalla tua banca, dall'Agenzia delle Entrate, da Poste o dall'INPS.
- ✕ Comunicare codici di verifica al telefono a chiunque, anche se dice di essere della banca.
- ✕ Reinstallare o formattare senza salvare le prove se vuoi denunciare.

Numeri utili

Italia	**112**
Svizzera	**112**
San Marino	**112**

I miei contatti: _____

Punto di ritrovo: _____

Cosa tenere a portata di mano

Base

- [ ] Autenticazione a due fattori su email e banca
- [ ] Password manager
- [ ] Backup di foto e documenti fuori dal computer **CONSIGLIATO**
- [ ] Contanti di riserva e numero della banca annotato su carta

Avanzato

- [ ] Chiavi di sicurezza fisiche (FIDO2) per gli account critici **CONSIGLIATO**
- [ ] Backup 3-2-1: tre copie, due supporti, una fuori casa **CONSIGLIATO**
- [ ] Router con firmware aggiornato e rete ospiti per gli apparecchi domestici
- [ ] Copia su carta dei codici di recupero

Dopo

- [ ] Attiva l'autenticazione a due fattori su email, banca, social e negozi online.
- [ ] Usa un password manager e password diverse per ogni servizio.
- [ ] Fai backup periodici su un disco che poi scolleghi.
- [ ] Tieni aggiornati sistema operativo e app.

modorifugio.it/playbook/attacco-informatico/ · Revisionato il 22 novembre 2026

Informazioni divulgative. Segui sempre le indicazioni della Protezione Civile e del 112.