



Studio Legale Giammatteo

AVVOCATI · VENAFRO

GUIDA PRATICA · EBOOK

Cybersicurezza

Riconoscere le minacce, proteggere dati e denaro, e reagire nel modo giusto quando qualcosa va storto. Una guida chiara per persone, professionisti e piccole imprese.

www.giammatteo.it

Via Nicandro Iosso, 6 — 86079 Venafro (IS)

studiolegale@giammatteo.it

— Introduzione

La sicurezza informatica non è un tema per soli tecnici: riguarda chiunque usi uno smartphone, una casella di posta o un conto online. La maggior parte degli attacchi non sfrutta sofisticate tecniche di intrusione, ma un errore umano — un clic affrettato, una password riutilizzata, un messaggio credibile al momento giusto.

Questa guida nasce dall'esperienza dello Studio nell'assistenza alle vittime di frodi informatiche e nella tutela dei dati. È pensata per essere letta in poco tempo e usata come promemoria pratico: nelle prime pagine spieghiamo come funzionano le minacce più comuni e come difendersi, sia come persone sia come piccole realtà professionali; nella seconda parte affrontiamo il profilo giuridico — quali reati vengono in rilievo e, soprattutto, cosa fare concretamente se si è colpiti.

L'obiettivo non è alimentare l'allarme, ma dare strumenti. Poche abitudini corrette riducono drasticamente il rischio; e sapere in anticipo come reagire fa la differenza tra un danno contenuto e uno grave.

COME LEGGERE QUESTA GUIDA

I riquadri chiari segnalano consigli operativi, quelli rossi gli errori da evitare, quelli verdi le buone pratiche consolidate. La checklist finale riassume tutto in una pagina, da tenere a portata di mano.

1 Le minacce più diffuse

Conoscere il “volto” degli attacchi è il primo passo per riconoscerli in tempo. Ecco quelli che incontriamo più spesso.

Phishing, smishing e vishing

Sono messaggi ingannevoli che imitano banche, corrieri, pubbliche amministrazioni o colleghi, per indurre a cliccare un link, aprire un allegato o comunicare credenziali e codici. Arrivano via e-mail (**phishing**), via SMS o messaggistica (**smishing**) o con una telefonata (**vishing**). Il tratto comune è la leva emotiva: urgenza (“il tuo conto sarà bloccato”), paura, o un'occasione da non perdere.

Furto di credenziali e “account takeover”

Una singola password scoperta o riutilizzata su più servizi può aprire l'accesso a e-mail, social, home banking e servizi di pagamento. Spesso le credenziali circolano dopo violazioni di siti terzi: chi le acquista prova le stesse combinazioni ovunque (tecnica del *credential stuffing*).

Ransomware e malware

Il **ransomware** è un programma che cifra i file del dispositivo o dell'azienda e chiede un riscatto per restituirli. Altri **malware** spiano ciò che si digita, sottraggono dati o trasformano il dispositivo in uno strumento al servizio dell'aggressore. Il contagio avviene tipicamente da un allegato, un programma scaricato da fonti non ufficiali o una vulnerabilità non aggiornata.

Truffe finanziarie e “BEC”

Comprendono le finte fatture, i falsi ordini di bonifico e la cosiddetta **BEC** (*Business Email Compromise*): l'aggressore, avendo compromesso o imitato una casella aziendale, chiede di modificare le coordinate di pagamento di un fornitore. Basta un IBAN cambiato all'ultimo momento per dirottare somme rilevanti.

Truffe affettive e cripto-truffe

Le frodi sentimentali (*romance scam*) e quelle sugli investimenti in criptovalute condividono uno schema: costruire fiducia nel tempo e poi indurre a versare denaro verso piattaforme o persone irraggiungibili. Lo Studio ha dedicato a questi temi guide specifiche; qui basti ricordare che nessun investimento serio garantisce rendimenti certi e che nessun partner conosciuto solo online dovrebbe chiedere denaro.

Violazioni di dati (“data breach”)

Quando i dati personali gestiti da un'azienda o da un servizio vengono sottratti o esposti, il rischio si sposta su clienti e utenti: gli stessi dati alimentano nuovi tentativi di phishing “su misura”, più credibili perché contengono informazioni reali.

2 Come proteggersi: le persone

Poche misure, applicate con costanza, fermano la grande maggioranza degli attacchi rivolti ai privati.

Password robuste e diverse per ogni servizio

Una password lunga e unica per ciascun account evita che la violazione di un sito comprometta tutto il resto. Ricordarle tutte è impossibile: per questo è utile un **gestore di password**, che le crea e le conserva in modo cifrato. È sufficiente ricordare una sola password principale, forte.

Attiva la verifica in due passaggi (2FA/MFA)

L'autenticazione a più fattori aggiunge, oltre alla password, un secondo elemento (un codice da app, una notifica, una chiave fisica). Anche se la password venisse scoperta, l'accesso resterebbe bloccato. Attivala su e-mail, home banking, servizi di pagamento e social: sono gli account più ambìti.

BUONA PRATICA

Preferisci i codici generati da un'app di autenticazione o una chiave fisica rispetto agli SMS: gli SMS possono essere intercettati o dirottati con il cambio fraudolento della SIM.

Aggiorna e fai il backup

Gli aggiornamenti chiudono le porte che i malware sfruttano: installali con tempestività su telefono, computer e applicazioni. In parallelo, tieni una copia di sicurezza dei dati importanti (foto, documenti) su un supporto o un servizio separato: è la migliore difesa contro il ransomware e i guasti.

Diffida dei link e degli allegati

Prima di cliccare, verifica il mittente e passa il puntatore sul link per leggerne il reale indirizzo. Nel dubbio, non cliccare: raggiungi il sito digitando tu l'indirizzo, o contatta l'ente con i recapiti ufficiali. Nessuna banca chiede per e-mail o SMS le credenziali complete o i codici di conferma.

ERRORE DA EVITARE

Comunicare codici OTP, PIN o password “per sbloccare” o “verificare” un pagamento. Chi te li chiede — anche al telefono, spacciandosi per operatore — sta tentando una truffa. Un operatore autentico non ne ha bisogno.

Attenzione a reti e dispositivi

Evita di svolgere operazioni sensibili su reti Wi-Fi pubbliche non protette; blocca smartphone e computer con codice o dati biometrici; non installare app o programmi da fonti non ufficiali.

3 Come proteggersi: professionisti e piccole imprese

Per uno studio o una piccola azienda valgono le stesse regole di base, con alcune attenzioni in più perché in gioco ci sono anche i dati dei clienti e la continuità del lavoro.

Le persone sono il primo firewall

La formazione periodica del personale sui segnali del phishing e sulle procedure di pagamento riduce il rischio più di qualsiasi tecnologia. Stabilisci una regola semplice e non derogabile: ogni variazione di IBAN o richiesta urgente di bonifico va verificata con un secondo canale (una telefonata al recapito noto del fornitore).

Accessi, ruoli e backup 3-2-1

Assegna a ciascuno solo i permessi necessari, revoca prontamente gli accessi di chi lascia l'organizzazione e adotta la verifica in due passaggi sugli strumenti aziendali. Per i backup vale la regola **3-2-1**: almeno tre copie dei dati, su due supporti diversi, di cui una conservata separatamente e non sempre collegata.

Un piano per il “giorno dopo”

Prepara in anticipo cosa fare in caso di incidente: chi isola i sistemi, chi avvisa i responsabili, come si comunica con clienti e autorità. Avere un piano scritto, anche breve, evita decisioni improvvisate nel momento peggiore.

IL QUADRO NORMATIVO PER LE IMPRESE

La direttiva europea NIS2 (Direttiva UE 2022/2555), recepita in Italia con il **D.lgs. 138/2024**, ha ampliato gli obblighi di sicurezza e di segnalazione degli incidenti per numerosi settori. Il punto di riferimento nazionale è l'**Agenzia per la Cybersicurezza Nazionale (ACN)**. Non tutte le piccole realtà vi rientrano, ma è opportuno verificare la propria posizione: lo Studio può aiutarti a inquadrarla.

4 La dimensione giuridica

Molte condotte informatiche costituiscono reato. Conoscerne l'inquadramento aiuta a capire quando e come rivolgersi all'Autorità.

I PRINCIPALI REATI INFORMATICI (CODICE PENALE)

Accesso abusivo a un sistema informatico o telematico — **art. 615-ter c.p.** · Detenzione, diffusione e installazione abusiva di codici e strumenti di accesso — **art. 615-quater c.p.** · Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche — **art. 617-quater c.p.** · Danneggiamento di informazioni, dati e programmi informatici — **art. 635-bis c.p.** · Frode informatica — **art. 640-ter c.p.** · Truffa — **art. 640 c.p.** · Sostituzione di persona — **art. 494 c.p.**

In concreto, un attacco può integrare più reati insieme: chi si impossessa delle credenziali per svuotare un conto risponde tipicamente di accesso abusivo e di frode informatica; chi crea un profilo falso a nome altrui per ingannare terzi può rispondere di sostituzione di persona. La qualificazione esatta dipende dai fatti, e incide anche sul regime di procedibilità e sui termini.

La protezione dei dati personali

Il trattamento dei dati è disciplinato dal **GDPR** (Regolamento UE 2016/679) e dal Codice in materia di protezione dei dati personali. Quando una violazione dei dati comporta un rischio per le persone, il titolare del trattamento deve **notificarla al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore** (artt. 33 e 34 GDPR); nei casi di rischio elevato va informato anche l'interessato. Per l'impresa colpita, gestire correttamente questa fase è tanto importante quanto risolvere l'incidente tecnico.

PERCHÉ DENUNCIARE CONVIENE

Anche quando recuperare il denaro sembra difficile, la denuncia o la querela avvia le indagini quando le tracce digitali sono ancora disponibili, permette di collegare episodi seriali e apre la strada alla costituzione di parte civile per il risarcimento del danno.

5 Sei stato colpito? Cosa fare

Nei primi minuti conta la lucidità. Ecco una sequenza ordinata, valida per la maggior parte dei casi.

1. Contieni il danno

Se sospetti un accesso non autorizzato, cambia immediatamente le password degli account coinvolti — a partire dall'e-mail, che è la chiave di tutto — e attiva la verifica in due passaggi. In caso di operazioni sospette sul conto, contatta senza indugio la banca per bloccare carte e disporre, ove possibile, lo storno o il richiamo del bonifico: la tempestività può fare la differenza.

2. Isola e non peggiorare

Se un dispositivo appare compromesso da ransomware o malware, scollegalo dalla rete e non spegnerlo forzatamente prima di aver chiesto assistenza: in alcuni casi lo stato del sistema è utile all'analisi. **Non pagare il riscatto di getto**: il pagamento non garantisce il recupero, alimenta il fenomeno e va valutato con un professionista.

3. Conserva le prove

Salva tutto ciò che documenta l'accaduto: schermate dei messaggi e delle pagine (con data e ora visibili), e-mail integrali, ricevute e contabili dei pagamenti, indirizzi, numeri, nickname e IBAN utilizzati. Sono elementi preziosi per le indagini e per un'eventuale azione risarcitoria.

DOVE RIVOLGERSI

Per i reati informatici il presidio specializzato è la **Polizia Postale e delle Comunicazioni**; la denuncia o la querela può essere presentata anche presso Carabinieri, Polizia di Stato o direttamente in Procura. Per i profili di protezione dei dati, il riferimento è il **Garante per la protezione dei dati personali**.

4. Denuncia o querela, nei termini

Alcuni reati procedono d'ufficio, altri richiedono la querela della persona offesa. Quando è necessaria, la querela va presentata **entro tre mesi** dal giorno in cui si è avuta conoscenza del fatto (art. 124 c.p.); le modalità sono disciplinate dagli artt. 336 e 337 c.p.p. Presentarla tempestivamente, anche contro ignoti, preserva i diritti e consente di attivare subito gli accertamenti.

5. Se sei un'azienda: valuta la notifica

Se la violazione ha interessato dati personali di clienti o dipendenti, valuta senza ritardo l'obbligo di notifica al Garante e, nei casi di rischio elevato, la comunicazione agli interessati. È una valutazione da compiere rapidamente e con criterio: un supporto legale nelle prime ore evita errori che pesano poi sul piano sanzionatorio e reputazionale.

6 Checklist essenziale

Per proteggerti

- ☐ Password lunga e diversa per ogni servizio, gestita con un password manager
- ☐ Verifica in due passaggi attiva su e-mail, banca, pagamenti e social
- ☐ Aggiornamenti installati con tempestività su tutti i dispositivi
- ☐ Backup regolare dei dati importanti, su un supporto separato
- ☐ Diffidenza verso link, allegati e richieste urgenti; nessun codice OTP condiviso
- ☐ Nelle attività: verifica di ogni cambio IBAN con un secondo canale; permessi minimi; piano di risposta scritto

Se sei stato colpito

- ☐ Cambia subito le password e blocca carte/conto con la banca
- ☐ Isola il dispositivo compromesso; non pagare riscatti d'impulso
- ☐ Conserva schermate, e-mail, ricevute, IBAN e ogni traccia utile
- ☐ Presenta denuncia/querela (Polizia Postale), nei termini di legge
- ☐ Se azienda: valuta la notifica del data breach al Garante entro 72 ore
- ☐ Fatti assistere presto: le prime ore sono decisive

UN PRINCIPIO DA RICORDARE

La sicurezza non è un prodotto che si compra una volta, ma un'abitudine. Piccoli gesti ripetuti — aggiornare, verificare, diffidare — proteggono più di qualsiasi soluzione miracolosa.

Hai subito un attacco o una truffa online?

Lo Studio Legale Giammatteo assiste persone e imprese nella tutela dopo un incidente informatico: dalla querela alla costituzione di parte civile, dalla gestione della violazione dei dati alle azioni per il recupero e la tutela della reputazione. Se hai un dubbio o un caso in corso, parlarne per tempo è già un vantaggio.

Studio Legale Giammatteo

Via Nicandro Iosso, 6 — 86079 Venafro (IS)

www.giammatteo.it · studiolegale@giammatteo.it

PEC: studiolegale@pec.giammatteo.it

Questa guida ha finalità informativa e divulgativa e non sostituisce una consulenza legale personalizzata sul caso concreto. I riferimenti normativi richiamati sono quelli in vigore alla data di redazione.