

Che cosa fare se succede

Quattro passi per reagire con calma quando l'incidente è già avvenuto

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa 3

1. Il momento in cui te ne accorgi 3

1.1 I segnali che qualcosa non va 4

2. I quattro passi, uno alla volta 5

2.1 Primo passo: isolare 5

2.2 Secondo passo: avvisare 6

2.3 Terzo passo: cambiare password e verifica in due passaggi 7

2.4 Quarto passo: conservare le prove e segnalare 9

3. Che cosa non fare 10

3.1 Gli errori più frequenti 11

4. Tre casi pratici 12

4.1 Caso 1: il link falso nella segreteria scolastica 12

4.2 Caso 2: il ransomware nello studio 13

4.3 Caso 3: la mail al destinatario sbagliato 13

5. Dopo l'incidente 13

5.1 Capire e ripristinare 14

5.2 Se sono coinvolti dati di persone 15

5.3 Imparare e migliorare 16

Esercitazione pratica 17

Le domande che arrivano in aula 18

Glossario 18

Per approfondire 19

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Sapere che cosa fare, e in che ordine, quando sospetti di aver cliccato un link falso, aperto un file pericoloso o perso dati: isolare, avvisare, cambiare password e verifica in due passaggi, conservare le prove e segnalare.

Che cosa saprai fare alla fine

- Riconoscere i segnali di un incidente e fermarsi invece di andare nel panico.
- Isolare un dispositivo sospetto dalla rete senza perdere le prove.
- Avvisare le persone giuste nell'ordine giusto, compresa la banca quando serve.
- Cambiare password e verifica in due passaggi partendo da un dispositivo pulito.
- Distinguere una segnalazione da una denuncia alla Polizia Postale e capire quando scatta la notifica al Garante.

1. Il momento in cui te ne accorgi

Prima o poi capita a tutti: un clic di troppo, un allegato aperto di fretta, uno schermo che si comporta in modo strano.

Immagina Marta, che lavora nella segreteria di una scuola. Riceve una mail che sembra della banca dell'istituto, clicca sul link, inserisce le credenziali e solo dopo nota che l'indirizzo della pagina era strano. Il cuore accelera. Cosa fa?

La reazione più comune è una di queste due: far finta di niente sperando che passi, oppure fare molte cose insieme e senza ordine. Sono entrambe sbagliate. Nel primo caso il problema cresce nel silenzio, nel secondo si rischia di cancellare proprio le tracce che servirebbero a capire che cosa è successo.

La buona notizia è che esiste una sequenza semplice, da imparare una volta sola. Sono quattro passi, sempre gli stessi, qualunque sia l'incidente.



Se succede: isola, avvisa, proteggi gli accessi, conserva e segnala

L'IDEA IN UNA RIGA

Prima fermi il danno, poi avvisi, poi metti in sicurezza gli accessi, infine conservi le prove e segnali.

1.1 I segnali che qualcosa non va

Non sempre l'incidente si annuncia con una schermata minacciosa. Spesso i segnali sono piccoli e vanno presi sul serio.

- hai cliccato un link o aperto un allegato e subito dopo succede qualcosa di insolito;
- i file hanno cambiato nome o estensione, oppure non si aprono più;
- compare un messaggio che chiede un riscatto in denaro;
- il computer è improvvisamente lentissimo o si comporta da solo;
- ti avvisano che dal tuo indirizzo di posta partono mail che non hai scritto;
- ricevi un avviso di accesso al tuo account da un luogo o da un dispositivo che non riconosci;
- vedi sul conto movimenti che non hai fatto.

IL DUBBIO BASTA

Non devi essere sicuro al cento per cento per agire. Se hai il sospetto di un incidente, comportati come se fosse vero e avvisa. Un falso allarme costa poco, un incidente taciuto costa molto.

2. I quattro passi, uno alla volta

Ecco la sequenza completa. Poi la vediamo con calma, passo per passo.

Passo	Che cosa fai	Perché
1. Isolare	Scolleghi il dispositivo dalla rete.	Il problema non si diffonde agli altri computer.
2. Avvisare	Dici subito che cosa è successo alla persona responsabile.	Chi ha gli strumenti può intervenire e proteggere gli altri.
3. Cambiare password e verifica	Cambi le password e controlli la verifica in due passaggi, da un dispositivo pulito.	Chi ha rubato le credenziali non può più usarle.
4. Conservare e segnalare	Tieni le prove e segnali alla Polizia Postale.	Servono per capire, per tutelarti e per le indagini.

I quattro passi da fare sempre, in questo ordine.

2.1 Primo passo: isolare

Isolare vuol dire togliere il dispositivo dalla rete. Se il computer è collegato con un cavo, scollegalo. Se usa il Wi-Fi, spegni il Wi-Fi dalle impostazioni rapide di Windows 11 oppure attiva la modalità aereo. In questo modo un eventuale programma dannoso non può né diffondersi agli altri computer dell'ufficio né comunicare con chi lo ha creato.

Se il dispositivo ha una chiavetta o un disco esterno collegato, scollega anche quelli: potrebbero essere i prossimi a essere colpiti. E se sospetti un ransomware (il programma che blocca i file e chiede un riscatto), scollegare in fretta può salvare le copie di backup, se erano collegate.

Poi lascia il computer com'è. Non formattarlo, non reinstallare niente e non cancellare file di tua iniziativa. Se il tuo ufficio ha un referente informatico, sarà lui a decidere come procedere.



Scollega la rete e chiedi assistenza, senza formattare

2.2 Secondo passo: avvisare

È il passo che costa di più, perché ci si vergogna. Eppure è il più importante. Più passa il tempo, più il danno si allarga: l'attaccante usa gli accessi che ha ottenuto per muoversi in altri sistemi, scrivere ai tuoi contatti o svuotare un conto.

Avvisa nell'ordine giusto. Prima il responsabile dell'ufficio o il referente informatico. Poi, se è stato coinvolto un conto o una carta, la banca, con il numero ufficiale che trovi sul sito o sul retro della carta (non quello scritto nella mail sospetta). Se la tua mail è stata usata per truffare altri, avvisa anche i tuoi contatti più importanti, con un messaggio breve: «Ignorate le mail strane arrivate dal mio indirizzo».



Avvisa il responsabile; se ci sono soldi coinvolti, chiama la banca al numero ufficiale

NON È UNA COLPA

Un buon ufficio premia chi segnala subito e non punisce chi sbaglia. La colpa vera è tacere.

2.3 Terzo passo: cambiare password e verifica in due passaggi

Se hai inserito una password in una pagina sospetta, quella password è da considerare compromessa. Cambiala subito sul sito vero (digitando tu l'indirizzo o usando un preferito, mai un link ricevuto). Poi cambia anche tutte le altre password che erano uguali o simili: chi ne ha una prova subito con gli altri servizi.

Fai il cambio da un dispositivo pulito, cioè da uno che non è quello sospetto: il tuo telefono, se non è coinvolto, o il computer di un collega. Se un programma spia (spyware) è rimasto sul computer, cambiare le password da lì le consegnerebbe di nuovo a chi ti spia.



Cambia le credenziali da un dispositivo affidabile e dal sito vero

Poi controlla la verifica in due passaggi (la seconda prova di identità, come il codice nell'app). Assicurati che sia attiva sugli account importanti: posta, banca, servizi dell'ente. Controlla anche che non siano comparsi dispositivi sconosciuti tra quelli autorizzati e, se il servizio lo permette, esci da tutte le sessioni aperte.



Controlla verifica in due passaggi, dispositivi autorizzati e inoltri sospetti

2.4 Quarto passo: conservare le prove e segnalare

Prima di cancellare la mail truffa, il messaggio o la schermata, conservane una copia: salva la mail come file, fai una fotografia dello schermo con il telefono, annota giorno, ora e che cosa hai fatto. Sono tue note, scritte a caldo: dopo una settimana non ti ricorderai nulla.



Conserva il messaggio, la foto dello schermo e giorno e ora

Poi segnala. In Italia il riferimento per i reati informatici è la **Polizia Postale e delle Comunicazioni**, la parte della Polizia di Stato che si occupa di crimini commessi online. Il suo portale, il Commissariato di Polizia di Stato online (commissariatodips.it), ti permette di scegliere tra più strade.



Una segnalazione non equivale a una denuncia formale

Strada	A che cosa serve
Segnalazione online	Porti all'attenzione della Polizia un comportamento che pensi illecito, così che possa verificarlo. Non è una denuncia.
Denuncia	È l'atto formale con cui racconti i fatti. Per i reati informatici il portale offre un servizio dedicato; puoi anche presentarla di persona a un ufficio di polizia.
Richiesta di informazioni	Se hai solo un dubbio, puoi chiedere consiglio agli esperti dal portale.

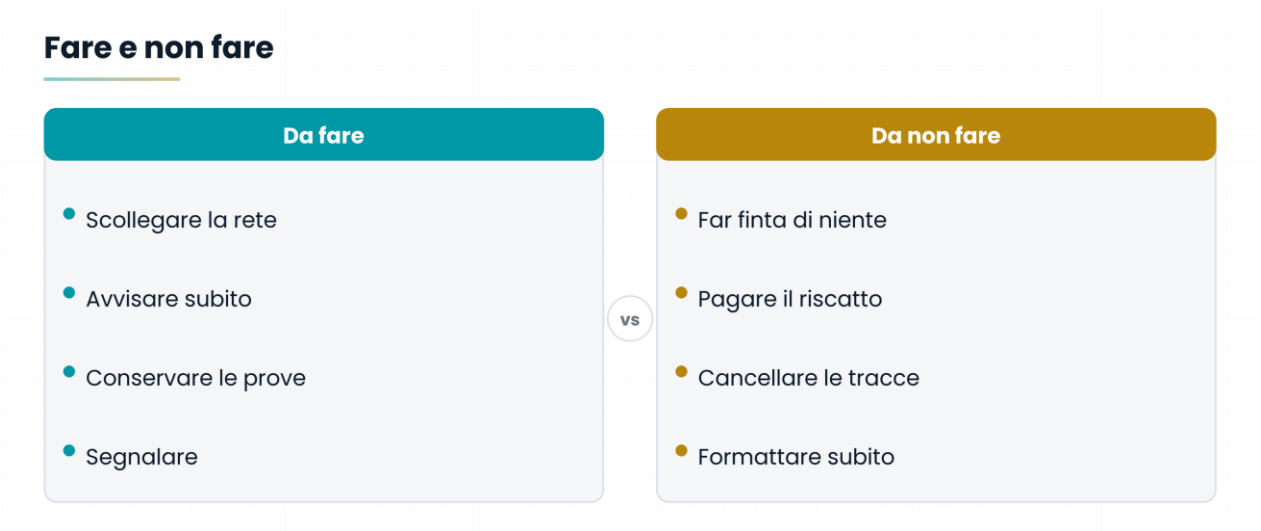
Le tre strade del portale della Polizia Postale.

SEGNALARE NON BASTA SE HAI PERSO SOLDI

La segnalazione online non sostituisce la denuncia e non è un servizio di emergenza. Se c'è un pericolo immediato chiama il 112 o il 113. Se hai perso denaro, chiama prima la banca e poi sporgi denuncia.

3. Che cosa non fare

Nel panico si fanno cose che sembrano utili e invece peggiorano la situazione.



Che cosa fare e che cosa non fare

3.1 Gli errori più frequenti

- **Far finta di niente.** Il silenzio è l'errore più costoso, perché dà tempo all'attaccante.
- **Pagare un riscatto.** Non c'è garanzia che i file tornino, e il pagamento finanzia altri attacchi e segna la tua azienda come cliente disponibile.
- **Rispondere ai ricattatori o richiamare il numero del messaggio.** Ogni risposta conferma che l'indirizzo è attivo.
- **Cancellare mail, file o cronologia** per «pulire». Distruggi le prove.
- **Formattare il computer subito.** Se lo fai prima di aver capito cosa è successo, non saprai cosa è stato rubato.
- **Cambiare le password dal computer infetto.** Le consegni di nuovo a chi ti spia.
- **Chiamare il numero scritto nella mail o nel messaggio** per «verificare». Cerca sempre il numero ufficiale tu.



Non tacere, non pagare, non cancellare le prove, non formattare da soli

ATTENZIONE AI FINTI SOCCORRITORI

Dopo un incidente può arrivare qualcuno che si offre di «recuperare tutto» in cambio di denaro, spesso contattandoti per primo. Se non l'hai cercato tu, diffida.

4. Tre casi pratici

La teoria è semplice. Vediamola applicata a tre situazioni da ufficio. I nomi sono di fantasia.

4.1 Caso 1: il link falso nella segreteria scolastica

Marta, della segreteria dell'Istituto Esempio, clicca su un link ricevuto per mail e inserisce le credenziali della posta. Si accorge che il dominio era sbagliato: ente-esempio.it diventava ente-esempio.com.

- **Isola:** chiude la pagina e scollega il computer dal Wi-Fi.
- **Avvisa:** lo dice subito al dirigente scolastico e al referente informatico, senza aspettare.
- **Cambia:** dal telefono cambia la password della posta e controlla che la verifica in due passaggi sia attiva; controlla le regole di inoltro, che gli attaccanti usano per ricevere copia della posta.

- **Conserva e segnala:** salva la mail truffa e annota l'ora; la scuola fa una segnalazione alla Polizia Postale.

Risultato: l'accesso è chiuso prima che l'attaccante lo usi. Marta non è stata punita, anzi: la scuola ha avvisato gli altri colleghi che stava circolando quella mail.

4.2 Caso 2: il ransomware nello studio

Al piccolo studio di consulenza Rossi e Soci, un lunedì mattina i file condivisi non si aprono più e compare un messaggio che chiede un pagamento. Giulia, la segretaria, non tocca nulla e non prova a «sistemare» da sola.

- **Isola:** scollega il cavo di rete e chiede a tutti di fare lo stesso; scollega anche il disco esterno dei backup.
- **Avvisa:** chiama il titolare e il tecnico di fiducia.
- **Cambia:** si cambiano da un dispositivo pulito le password della posta e dei servizi online.
- **Conserva e segnala:** si fotografa il messaggio del riscatto e si presenta denuncia alla Polizia Postale.

Lo studio non paga. Il disco di backup era scollegato dalla settimana prima, perciò il tecnico ripristina i dati dall'ultima copia sana. Si perdono alcuni giorni di lavoro, non tutto. Qui si vede perché la lezione sul backup è la vera assicurazione.

4.3 Caso 3: la mail al destinatario sbagliato

In un ufficio, Luca invia per errore a un indirizzo esterno un elenco con nomi, codici fiscali e dati di contatto di alcune persone. Non c'è nessun attaccante, ma è comunque una violazione dei dati personali.

Che cosa fa? Avvisa subito il titolare del trattamento (cioè chi decide come si usano i dati dell'ente). Prova a richiamare il messaggio e chiede al destinatario, per iscritto, di cancellarlo senza aprirlo. Annota che cosa è successo. Sarà il titolare a valutare se sia necessario notificare la violazione al Garante, come vediamo nell'ultima sezione.

5. Dopo l'incidente

Quando l'emergenza è passata, resta il lavoro più utile: capire e migliorare. Un incidente gestito bene è una lezione che costa meno di quella che arriverebbe la volta dopo.



Dopo l'incidente: dal ripristino al miglioramento

5.1 Capire e ripristinare

Insieme al referente informatico ricostruite i fatti: che cosa è stato colpito, che cosa è stato visto o portato via, da dove è entrato l'attaccante. Solo dopo si ripristina, con i backup e su un sistema ripulito. Ripristinare prima di aver chiuso la porta d'ingresso significa ricevere lo stesso attacco una seconda volta.



Capisci la causa, chiudi l'accesso, ripristina su un sistema pulito, migliora

5.2 Se sono coinvolti dati di persone

Quando l'incidente riguarda dati personali, entra in gioco il GDPR (il regolamento europeo sulla protezione dei dati) e scatta il dovere di valutare la violazione. A farlo è il **titolare del trattamento**, non il singolo dipendente: tu avvisi subito, lui decide.

- la violazione va notificata al Garante per la protezione dei dati personali, l'autorità italiana che controlla la privacy, **senza ingiustificato ritardo e, ove possibile, entro 72 ore** da quando il titolare ne è venuto a conoscenza;
- la notifica non serve se è improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone;
- la notifica oltre le 72 ore è possibile, ma bisogna spiegare i motivi del ritardo;
- oggi la notifica si fa con la procedura telematica sul sito del Garante;
- se il rischio per le persone è elevato, vanno informati anche gli interessati, cioè le persone a cui i dati si riferiscono;
- ogni violazione va comunque annotata in un registro interno, anche quando non viene notificata.



Il titolare valuta il rischio, notifica e informa le persone quando serve

IL TEMPO COMINCIA SUBITO

Le 72 ore contano da quando il titolare ne ha avuto conoscenza. Per questo è così importante che tu avvisi subito: se tieni il problema per te, fai perdere tempo prezioso a tutta l'organizzazione.

5.3 Imparare e migliorare

Chiudi con un breve confronto, senza cercare colpevoli. Che cosa ha permesso l'incidente? Una password debole, un aggiornamento rimandato, un backup mai provato? Scegli una o due azioni concrete e fissa chi le farà. Poi racconta l'accaduto ai colleghi: un incidente ben raccontato ai colleghi vale più di mille avvisi generici.

DOPO IL CASO DELLA SCUOLA

Dopo la mail falsa, l'Istituto Esempio attiva la verifica in due passaggi sulle caselle di tutta la segreteria e prepara una scheda con i quattro passi da appendere accanto al telefono.



Scrivi il promemoria e i contatti prima che servano

Esercitazione pratica

Una breve esercitazione per preparare, adesso e con calma, il piano che ti servirà se un giorno ti trovi nei guai.

1. Prendi un foglio e scrivi in alto «Se succede». Sotto, elenca i quattro passi con parole tue.
2. Accanto al passo «Avvisare», scrivi il nome e il numero della persona da chiamare nel tuo ufficio o in famiglia.
3. Cerca sul sito ufficiale della tua banca il numero per bloccare carte e conti e annotalo sul foglio.
4. Apri commissariatodips.it e guarda dove si trovano la segnalazione online e la denuncia per reati telematici; annota l'indirizzo.
5. Prova a trovare nelle impostazioni rapide di Windows 11 il pulsante per spegnere il Wi-Fi o attivare la modalità aereo.
6. Appendi il foglio vicino alla postazione o salvalo in un posto sicuro.

CONTROLLA DI AVER FATTO COSÌ

Il foglio contiene almeno un nome e un numero da chiamare?

Sai come scollegare il tuo computer dalla rete?

Il numero della banca viene dal sito ufficiale e non da una mail?

Le domande che arrivano in aula

Ho cliccato un link ma non è successo niente. Devo fare qualcosa?

Sì, almeno avvisare e controllare. Alcuni programmi dannosi non si vedono. Scollega il dispositivo, avvisa il referente, cambia la password se l'hai inserita e controlla gli accessi recenti all'account.

Posso spegnere il computer subito?

Scollegarlo dalla rete è la prima cosa. Spegnerlo è una scelta che dipende dal caso: chiedi al referente informatico. L'importante è non formattarlo né reinstallare nulla prima di aver capito cosa è successo.

Devo per forza denunciare alla Polizia Postale?

Se hai subito un danno, per esempio una truffa con perdita di denaro o un furto di identità, conviene denunciare. In altri casi puoi inviare una segnalazione online. Se hai dubbi, il portale permette di chiedere informazioni.

La notifica al Garante tocca a me?

No, spetta al titolare del trattamento, cioè chi decide come si usano i dati dell'ente. Il tuo compito è avvisarlo subito, perché i termini partono da quando lui ne viene a conoscenza.

Posso pagare il riscatto se non ho il backup?

È sconsigliato. Non c'è garanzia di riavere i file e si finanziano altri attacchi. Prima di decidere fai valutare il caso a un tecnico e valuta la denuncia.

Come faccio a sapere se mi hanno rubato i dati?

Non sempre si può sapere subito. Controlla gli accessi recenti agli account, gli avvisi della banca e le regole di inoltro della posta. In caso di dubbio chiedi aiuto a un tecnico.

Glossario

Termine	Che cosa significa
Denuncia	L'atto formale con cui si racconta un reato all'autorità.
Garante per la protezione dei dati personali	L'autorità italiana indipendente che controlla il rispetto della privacy.

Termine	Che cosa significa
Incidente di sicurezza	Un evento che mette a rischio la riservatezza, l'integrità o la disponibilità dei dati.
Isolare	Scollegare un dispositivo dalla rete, con il cavo o spegnendo il Wi-Fi, per fermare la diffusione di un problema.
Polizia Postale e delle Comunicazioni	La parte della Polizia di Stato che si occupa dei reati informatici. Il portale è commissariatodips.it.
Prove	Mail, schermate e appunti che documentano che cosa è successo e che servono per capire e per denunciare.
Segnalazione	Comunicazione alla Polizia di un fatto che sembra illecito, perché lo verifichi. Non sostituisce la denuncia.
Titolare del trattamento	Chi decide perché e come si usano i dati personali, per esempio l'ente, lo studio o l'azienda.
Violazione dei dati personali	Un incidente che porta alla perdita, alla modifica, alla diffusione o all'accesso non autorizzato a dati di persone.

Per approfondire

Commissariato di Polizia di Stato online (Polizia Postale e delle Comunicazioni), commissariatodips.it - segnalazione online, denuncia per reati telematici, informazioni; consultato a ottobre 2026

Garante per la protezione dei dati personali, pagina sulle violazioni di dati personali (data breach) - termine di 72 ore, procedura telematica, registro interno; consultato a ottobre 2026

Regolamento (UE) 2016/679 (GDPR), articoli 33 e 34 - notifica all'autorità di controllo e comunicazione agli interessati

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. I servizi dei siti della Polizia Postale e del Garante possono cambiare: controlla sempre le pagine ufficiali. Questa lezione è una guida generale e non sostituisce il parere di un tecnico o di un legale.