*Materia: INFORMATICA*

# Sicurezza informatica 3 - Incidenti, backup e protezione dei dati

*Riconoscere problemi, reagire con metodo, proteggere i dati e verificare il ripristino*

Una buona sicurezza non consiste soltanto nel prevenire problemi. Occorre anche riconoscere i segnali di un possibile incidente, reagire in modo ordinato e prepararsi a recuperare i dati dopo un guasto, un errore o un attacco. In azienda la regola più importante è semplice: non improvvisare.

| IDEA FONDAMENTALE |
| --- |
| Un incidente informatico non si affronta con il panico né con tentativi casuali. Prima si osserva, poi si segnala, si isola ciò che è necessario e si recupera dai backup verificati. |

## 1. Un sintomo non è ancora una diagnosi

Un computer lento non è necessariamente infetto. Potrebbe avere poco spazio disponibile, troppi programmi aperti oppure un aggiornamento in corso. Tuttavia, più segnali contemporaneamente richiedono attenzione. L'obiettivo non è spaventarsi, ma osservare e segnalare in modo preciso.

La differenza tra un piccolo problema e un incidente vero non è sempre immediata. Per questo è importante imparare a descrivere bene ciò che accade: che cosa si stava facendo, quale messaggio è comparso, quando è iniziato il problema e quali file o account sembrano coinvolti.


*Figura 1 - Possibili segnali da osservare su dispositivi e account.*

## 2. Segnali possibili sul dispositivo

Alcuni segnali possono indicare un problema tecnico, un errore di configurazione o una possibile infezione. Presi da soli non bastano sempre per una diagnosi, ma devono essere valutati con attenzione.

- rallentamenti improvvisi e persistenti;
- finestre pubblicitarie inattese;
- reindirizzamenti del browser;
- applicazioni sconosciute;
- antivirus o protezioni disattivati;
- file rinominati, cifrati o non più accessibili;
- consumo anomalo di batteria o traffico dati come indizio da valutare;
- messaggi di riscatto o richieste di pagamento.

## 3. Segnali possibili sugli account

Un incidente può riguardare anche un account, non soltanto un computer. In questo caso i segnali arrivano spesso da notifiche, email automatiche o comportamenti anomali del profilo.

- password modificata senza autorizzazione;
- email, messaggi o post inviati automaticamente;
- accessi da dispositivi o luoghi sconosciuti;
- notifiche di recupero password non richieste;
- numero di telefono o email di recupero cambiati;
- movimenti bancari oppure acquisti anomali.

## 4. Che cosa fare a casa

Se sospetti un problema, interrompi le attività delicate. Non accedere all'home banking dal dispositivo sospetto e non inserire nuove password. Se il comportamento è molto anomalo, scollega il dispositivo dalla rete e chiedi aiuto a una persona competente.

Quando devi controllare gli account più importanti, usa un altro dispositivo affidabile. Se il dispositivo sospetto contiene malware, cambiare la password proprio da lì potrebbe consegnare anche la nuova credenziale all'attaccante.

## 5. Che cosa fare a scuola o in azienda

In un'organizzazione non bisogna tentare soluzioni casuali, cancellare file o formattare il computer. È importante segnalare rapidamente l'accaduto al docente, al tecnico o al referente informatico. Conservare messaggi, schermate e informazioni può aiutare a ricostruire l'incidente.

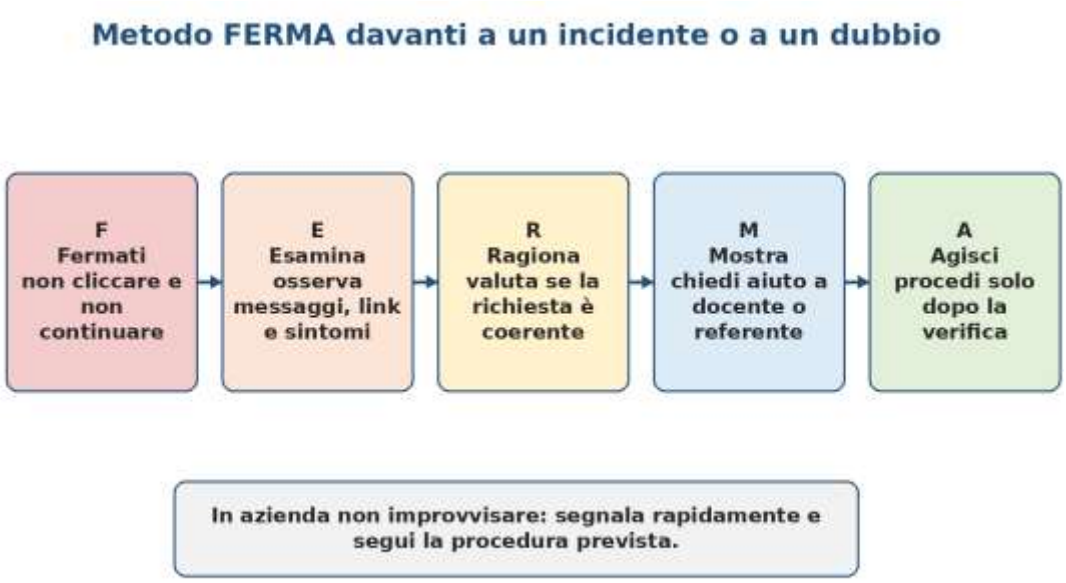


*Figura 2 - Metodo FERMA per reagire con ordine a un dubbio o a un incidente.*

| REGOLA AZIENDALE |
| --- |
| Interrompi l'attività rischiosa. Isola il dispositivo soltanto secondo la procedura prevista. Non cancellare file e non tentare riparazioni improvvisate. Contatta subito il referente informatico. |

## 6. Ransomware e importanza delle copie offline

Il ransomware tenta di rendere inaccessibili i dati e può cercare anche le copie raggiungibili dalla rete. Per questo una copia sempre collegata al computer non offre la stessa protezione di una copia scollegabile oppure offline. Pagare un riscatto non garantisce il recupero dei file e non deve essere una decisione improvvisata.

La protezione vera nasce prima dell'incidente: copie separate, account protetti, controlli periodici e procedure chiare. Quando il ransomware è già entrato, ogni minuto conta, ma improvvisare può peggiorare la situazione.

## 7. Che cos'è un backup

Il backup è una copia dei dati creata per poterli recuperare. Non basta copiare un file una sola volta: bisogna decidere quali dati proteggere, con quale frequenza eseguire le copie e dove conservarle. Il restore è l'operazione con cui i dati vengono ripristinati da una copia di sicurezza.

| Concetto | Significato pratico |
|---|---|
| Backup | copia dei dati preparata per il recupero; |
| Restore | ripristino dei dati da una copia di sicurezza; |
| Verifica | controllo che la copia sia leggibile e davvero recuperabile; |
| Versione | copia precedente utile se un file viene modificato o cancellato per errore. |

## 8. Strategia 3-2-1

La regola 3-2-1 suggerisce di mantenere tre copie dei dati, utilizzare almeno due tipi di supporto e conservare una copia fuori sede oppure offline. Non è l'unica strategia possibile, ma è un riferimento molto utile per comprendere il principio della ridondanza.


*Figura 3 - Strategia di backup 3-2-1.*

## 9. Tipi di backup

| Tipo | Vantaggi | Attenzioni |
|---|---|---|
| Locale | rapido e semplice; | può essere colpito dallo stesso guasto del dispositivo; |
| Disco esterno scollegabile | utile contro molti problemi e facile da conservare; | deve essere scollegato e custodito correttamente; |
| Cloud | accessibile da più luoghi e dispositivi; | richiede account protetto, condivisioni corrette e connessione; |
| NAS | utile in rete domestica o aziendale; | non sostituisce automaticamente una copia offline; |
| Offline o fuori sede | riduce il rischio che un singolo incidente colpisca tutte le copie; | deve essere aggiornata e verificata periodicamente. |

## 10. Verificare il restore

Un backup che non è mai stato provato può essere incompleto, danneggiato oppure inutilizzabile. È quindi necessario verificare periodicamente il restore: scegliere alcuni file, recuperarli in una posizione di prova e controllare che siano leggibili. La verifica deve essere pianificata, non rimandata al giorno dell'emergenza.

| DA RICORDARE |
| --- |
| La domanda non è soltanto "ho una copia?", ma "sono davvero in grado di recuperare i dati quando mi servono?". Un backup non verificato è una promessa, non una certezza. |

## 11. Proteggere home banking e documenti sensibili

Per l'home banking usa l'app ufficiale oppure un indirizzo noto digitato direttamente. Non seguire link ricevuti via email o SMS, non comunicare codici temporanei e controlla periodicamente i movimenti. I documenti sensibili devono essere conservati soltanto quando necessario, in spazi protetti. Una cassaforte virtuale cifrata può essere utile, ma deve essere configurata correttamente.

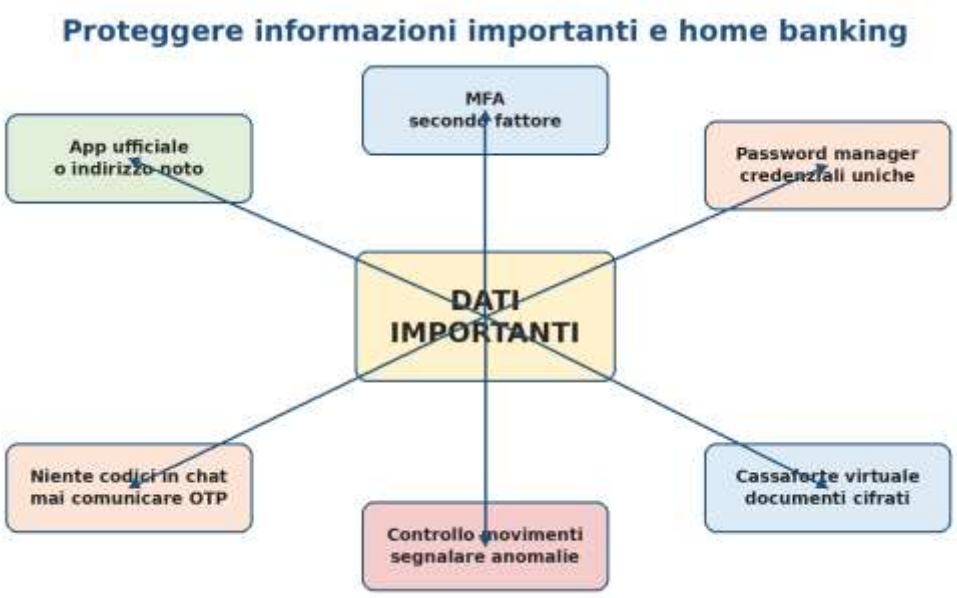


*Figura 4 - Protezione delle informazioni importanti e dell'home banking.*

## 12. Condivisioni cloud e dati riservati

Prima di condividere un file nel cloud, controlla chi può visualizzarlo e chi può modificarlo. Un collegamento pubblico può essere comodo, ma non è adatto a documenti riservati. In azienda e a scuola bisogna rispettare le regole definite dall'organizzazione.

## 13. Preparare una piccola strategia personale

Uno studente può iniziare proteggendo documenti scolastici, fotografie importanti e credenziali. Una strategia semplice potrebbe prevedere: file originale sul computer, copia periodica su disco esterno scollegato e copia cloud protetta mediante MFA. L'importante è non lasciare che l'unica copia viva nello stesso dispositivo che potrebbe rompersi o essere smarrito.

## 14. Sincronizzazione e backup

La sincronizzazione mantiene aggiornati gli stessi file su più dispositivi. È comoda, ma una cancellazione oppure una modifica sbagliata può propagarsi rapidamente. Il backup ha uno scopo diverso: conservare copie recuperabili. Alcuni servizi cloud offrono versioni precedenti e cestino, ma la strategia di protezione deve essere pensata consapevolmente.


*Figura 5 - Sincronizzazione e backup hanno obiettivi differenti.*

## 15. Frequenza, versioni e conservazione

Non tutti i dati richiedono la stessa frequenza di copia. Un documento su cui lavori ogni giorno merita backup più frequenti di un file che non cambia mai. Conservare alcune versioni precedenti può aiutare a recuperare un contenuto modificato per errore. La durata di conservazione dipende dal valore del dato e dalle regole dell'organizzazione.

## 16. Informazioni utili da segnalare durante un incidente

Quando segnali un problema, descrivi con precisione che cosa stavi facendo, quale messaggio è comparso, a che ora, quali file risultano coinvolti e se hai già cliccato, aperto allegati oppure inserito credenziali. Non nascondere un errore per vergogna: una segnalazione rapida riduce i danni.

| Informazione | Perché è utile |
|---|---|
| Ora e contesto | aiuta a ricostruire la sequenza degli eventi; |
| Messaggio visualizzato | permette di capire se si tratta di errore, truffa o infezione; |
| File o account coinvolti | indica quali dati devono essere protetti per primi; |
| Azioni già compiute | consente al referente di valutare il rischio reale. |

## 17. Piccolo piano personale di continuità

Per i file più importanti prepara una struttura semplice: cartella ordinata sul computer, copia su supporto esterno scollegato, copia cloud protetta e controllo periodico del ripristino. Per gli account principali conserva recapiti di recupero aggiornati e MFA attiva. In caso di smarrimento del telefono, devi sapere come bloccare o recuperare gli accessi.

## 18. Glossario essenziale

| Termine | Significato |
|---|---|
| Incidente | evento che può compromettere dati, dispositivi o account; |
| Backup | copia creata per recuperare dati; |
| Restore | ripristino da una copia; |
| Offline | non normalmente raggiungibile dalla rete; |
| Ransomware | malware che blocca o cifra dati; |
| Ridondanza | presenza di più copie o risorse; |

| | |
|---|---|
| NAS | dispositivo di archiviazione collegato alla rete; |
| Sincronizzazione | allineamento dei file tra dispositivi; |
| Versioning | conservazione di versioni precedenti; |
| Continuità operativa | capacità di proseguire o riprendere il lavoro dopo un problema. |

## 19. Sintesi operativa

Riconoscere un incidente significa osservare senza panico e reagire con metodo. A casa bisogna interrompere le attività delicate e chiedere aiuto. In azienda bisogna seguire la procedura e segnalare rapidamente. I backup devono essere multipli, separati e verificati. La domanda corretta non è soltanto “ho fatto una copia?”, ma “sono davvero in grado di recuperare i dati quando servono?”.

## 20. Domande di verifica

Rispondi con parole tue. Le domande servono a verificare la comprensione, non a ripetere meccanicamente il testo.

1. Perché un singolo rallentamento non dimostra la presenza di malware?
2. Quali segnali sul dispositivo richiedono attenzione?
3. Quali segnali possono indicare la violazione di un account?
4. Che cosa devi evitare su un dispositivo sospetto?
5. Perché conviene usare un altro dispositivo affidabile per cambiare password?
6. Che cosa devi fare in azienda davanti a un sospetto incidente?
7. Perché non devi formattare subito il computer aziendale?
8. Che cos’è il ransomware?
9. Perché una copia sempre collegata può essere rischiosa?
10. Che cos’è un backup?
11. Che cos’è il restore?
12. Che cosa significa strategia 3-2-1?
13. Qual è la differenza tra backup locale e copia offline?
14. Perché un NAS non sostituisce automaticamente una copia offline?
15. Perché bisogna verificare periodicamente il restore?
16. Come devi accedere all’home banking?
17. Perché non devi comunicare codici temporanei?
18. Che cos’è una cassaforte virtuale?
19. Che cosa devi controllare prima di condividere un file nel cloud?
20. Quale strategia semplice può adottare uno studente per i file importanti?

## 21. Risposte ragionate

1. Perché può dipendere da molte cause normali, come poco spazio, programmi aperti o aggiornamenti.
2. Popup inattesi, app sconosciute, reindirizzamenti, antivirus disattivato, file cifrati e messaggi di riscatto.
3. Password cambiate, accessi sconosciuti, messaggi inviati automaticamente, recapiti di recupero modificati e acquisti anomali.
4. Evitare pagamenti, inserimento di nuove credenziali e tentativi casuali di riparazione.
5. Perché il dispositivo sospetto potrebbe intercettare le nuove credenziali.
6. Interrompere il lavoro rischioso, seguire la procedura e contattare rapidamente il referente informatico.
7. Perché si potrebbero perdere informazioni utili per capire che cosa è accaduto e recuperare dati.
8. È un malware che blocca o cifra dati e tenta di ottenere un riscatto.
9. Perché alcuni ransomware cercano e colpiscono anche copie accessibili dalla rete o dal dispositivo.
10. È una copia dei dati creata per poterli recuperare.
11. È l’operazione di ripristino dei dati da una copia di sicurezza.
12. Tre copie dei dati, due tipi di supporto e una copia fuori sede oppure offline.
13. Il backup locale è vicino al dispositivo; la copia offline non è normalmente raggiungibile dalla rete.
14. Perché può restare raggiungibile dalla rete e subire lo stesso incidente.
15. Perché una copia non verificata potrebbe risultare incompleta o illeggibile proprio quando serve.

16. Mediante app ufficiale oppure indirizzo noto, evitando link inattesi.
17. Perché possono permettere a un attaccante di completare un accesso o un pagamento.
18. È uno spazio protetto e cifrato usato per conservare documenti o informazioni sensibili.
19. Chi può visualizzare, modificare e condividere il file; evitare collegamenti pubblici non necessari.
20. Conservare file originale, copia su disco esterno scollegato e copia cloud protetta con MFA.

## 22. Esercizi pratici e attività

Le attività devono essere svolte su scenari simulati o su file di prova. Non usare dati personali reali e non modificare impostazioni di sicurezza senza autorizzazione.

1. Analizza un elenco di sintomi e separa quelli deboli da quelli urgenti.
2. Prepara una checklist di azioni da compiere a casa davanti a un sospetto incidente.
3. Prepara una checklist diversa per la scuola o l'azienda.
4. Applica il metodo FERMA a un messaggio di riscatto simulato.
5. Disegna uno schema della strategia 3-2-1 per i file scolastici.
6. Individua tre file personali che meritano un backup.
7. Crea una cartella di prova e copiala su un supporto autorizzato.
8. Simula il restore di alcuni file in una cartella diversa.
9. Scrivi la differenza tra disco esterno sempre collegato e disco esterno scollegabile.
10. Spiega perché una copia cloud deve essere protetta con MFA.
11. Analizza tre scenari di condivisione cloud e scegli l'autorizzazione corretta.
12. Prepara una guida breve per proteggere l'home banking.
13. Elenca cinque informazioni da non inviare tramite chat.
14. Progetta una strategia mensile di backup per uno studente.
15. Scrivi una segnalazione sintetica da inviare a un referente informatico.

## 23. Checklist finale

| CHECKLIST FINALE |
| --- |
| Segnali osservati con calma. Attività delicate interrotte. Nessuna riparazione improvvisata. Referente avvisato. Account importanti controllati da dispositivo affidabile. Backup multipli, separati e verificati. Restore provato periodicamente. |