Materia: INFORMATICA

Sicurezza informatica 1 - Minacce, phishing e trappole digitali

Malware, ingegneria sociale, messaggi sospetti, QR code, USB sconosciute e comportamento prudente

La sicurezza informatica non riguarda soltanto i tecnici o le grandi aziende. Ogni persona che utilizza uno smartphone, un computer, una casella di posta elettronica o un servizio online deve imparare a riconoscere situazioni anomale e a comportarsi con prudenza. Molti attacchi riescono non perché la tecnologia sia completamente priva di difese, ma perché qualcuno convince l'utente a fare una scelta sbagliata.

IDEA FONDAMENTALE
Un utente prudente non deve sapere tutto: deve saper rallentare, controllare, chiedere aiuto e non agire d'impulso quando qualcosa sembra strano.

1. Sicurezza informatica: proteggere persone, dati e dispositivi

La sicurezza informatica è l'insieme delle regole, delle abitudini e degli strumenti utilizzati per proteggere dati, account, dispositivi e reti. I file scolastici, le fotografie, i messaggi, le credenziali e i dati bancari hanno un valore. Anche un account di gioco o un profilo social può essere usato per truffare amici e parenti, diffondere messaggi offensivi oppure danneggiare la reputazione della vittima.

Essere prudenti non significa vivere con paura. Significa fermarsi quando qualcosa non torna, controllare prima di agire e chiedere aiuto quando non si è sicuri. In informatica la velocità è utile, ma la fretta è spesso una pessima consigliera.

2. Malware: programmi creati per causare danni

Con il termine malware si indicano programmi o componenti software progettati per danneggiare un dispositivo, rubare informazioni, spiare l'utente, mostrare pubblicità indesiderata oppure impedire l'accesso ai file. Non tutti i malware si comportano allo stesso modo.

Minaccia	**Caratteristiche essenziali**	**Possibili conseguenze**
Virus	si collega ad altri file e si attiva quando il file viene eseguito;	può alterare o danneggiare file e programmi;
Worm	si propaga autonomamente attraverso reti e sistemi;	può diffondersi rapidamente tra molti dispositivi;
Trojan	si presenta come un programma utile oppure innocuo;	può aprire accessi non autorizzati o installare altro malware;
Spyware	raccoglie informazioni senza autorizzazione;	può violare privacy e riservatezza;
Keylogger	registra ciò che viene digitato;	può intercettare password e messaggi;
Ransomware	blocca o cifra file e sistemi;	può rendere inaccessibili documenti e fotografie;
Adware	mostra pubblicità indesiderata;	può rallentare il dispositivo e disturbare l'uso normale.

Figura 1 - Panoramica semplificata delle principali minacce informatiche.

3. Aggiornamenti, antivirus e firewall

Gli aggiornamenti correggono errori e vulnerabilità. Una vulnerabilità è un difetto che potrebbe essere sfruttato da un attaccante. È importante aggiornare il sistema operativo, il browser, le app e i programmi utilizzati per aprire documenti. Anche antivirus e firewall contribuiscono alla protezione, ma nessun singolo strumento garantisce una sicurezza assoluta.

REGOLA PRATICA
Installa programmi e aggiornamenti soltanto da fonti affidabili. Non disattivare antivirus o protezioni perché una finestra Web ti invita a farlo. Se un messaggio dice che il computer è infetto e chiede di fare clic immediatamente, fermati e verifica.

4. Ingegneria sociale: attaccare la fiducia della persona

L'ingegneria sociale è l'insieme delle tecniche usate per convincere una persona a rivelare informazioni o compiere azioni rischiose. L'attaccante può fingere di essere un tecnico, una banca, un corriere, un docente oppure un conoscente. L'obiettivo è indurre l'utente a fare clic, installare un programma, comunicare una password o inviare denaro.

Le leve più comuni sono fretta, paura, curiosità, promessa di un premio, senso di autorità e richiesta di segretezza. Quando un messaggio spinge a decidere subito, è proprio il momento di rallentare.

Figura 2 - Alcune leve psicologiche sfruttate dagli attacchi di ingegneria sociale.

5. Phishing, smishing e vishing

Il phishing è una truffa in cui un messaggio oppure un sito imitano un soggetto affidabile. Lo smishing usa SMS o messaggi sul telefono. Il vishing usa invece telefonate o messaggi vocali. Cambia il canale, ma il meccanismo è simile: l'attaccante prova a ottenere dati, denaro o accesso al dispositivo.

Un messaggio sospetto può parlare di un pacco bloccato, di un conto bancario da verificare, di una multa, di un premio oppure di un account in scadenza. Non basta osservare il logo: un logo può essere copiato facilmente. Bisogna controllare il mittente, l'indirizzo completo, la richiesta ricevuta e il dominio del sito verso cui porta il link.

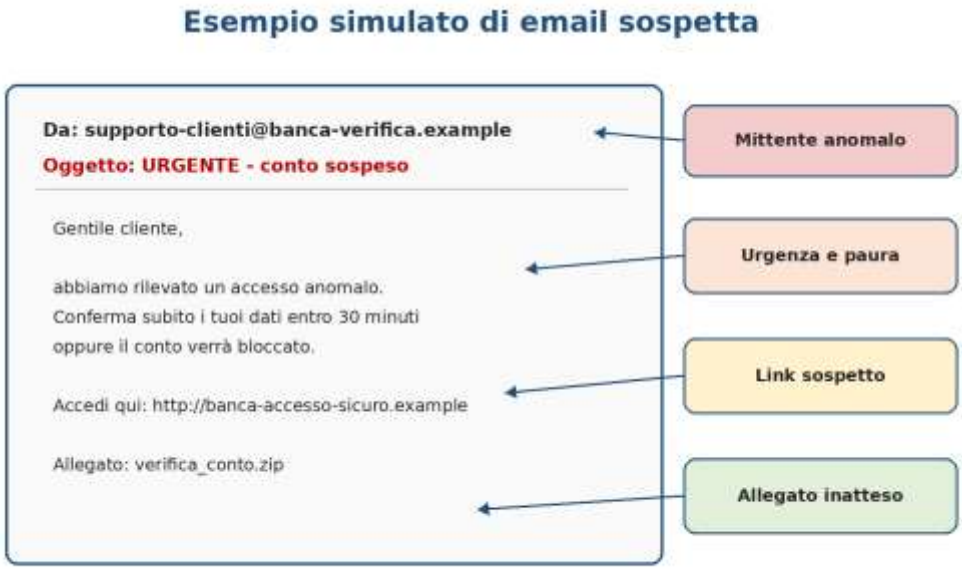

Figura 3 - Email simulata con alcuni segnali tipici di phishing.

6. Come comportarsi davanti a un messaggio sospetto

Davanti a un messaggio inatteso, soprattutto se chiede credenziali, denaro, allegati o azioni urgenti, è utile seguire una sequenza prudente.

- non fare clic immediatamente sui link;

- non aprire allegati inattesi;
- controlla l'indirizzo completo del mittente;
- non comunicare password, PIN o codici temporanei;
- accedi ai servizi importanti digitando manualmente l'indirizzo noto oppure usando l'app ufficiale;
- verifica mediante un secondo canale, per esempio un numero di telefono già conosciuto;
- a scuola o in azienda segnala il messaggio secondo la procedura prevista.

7. Siti imitati, risultati sponsorizzati e download

Un sito falso può imitare colori, logo e grafica del sito autentico. Per questo è necessario leggere con attenzione il dominio nella barra degli indirizzi. Anche i risultati sponsorizzati nei motori di ricerca richiedono prudenza: possono essere legittimi, ma non devono essere considerati automaticamente affidabili solo perché appaiono in evidenza.

Quando devi scaricare un programma, usa lo store ufficiale oppure il sito del produttore. Evita portali poco chiari, versioni pirata e finestre che promettono aggiornamenti miracolosi. Prima di aprire un file, controlla nome, estensione e provenienza.

8. QR code: comodi ma poco trasparenti

Un QR code consente di aprire rapidamente un collegamento. Il problema è che il collegamento non è immediatamente visibile. Un adesivo può essere sovrapposto a quello originale su un manifesto, un parchimetro o una bacheca. Prima di aprire il sito, leggi l'indirizzo visualizzato dallo smartphone. Se il QR code riguarda un pagamento o richiede credenziali, usa ancora più prudenza.

9. Chiavette USB, cavi e dispositivi sconosciuti

Una chiavetta USB trovata per terra oppure inserita in un punto pubblico non deve essere collegata al proprio computer. Può contenere file dannosi oppure comportarsi come un dispositivo progettato per inviare comandi. In alcune città esistono USB dead drops, nate come progetto artistico di scambio anonimo di file: dal punto di vista della sicurezza, non sono adatte a un dispositivo personale, scolastico o aziendale.

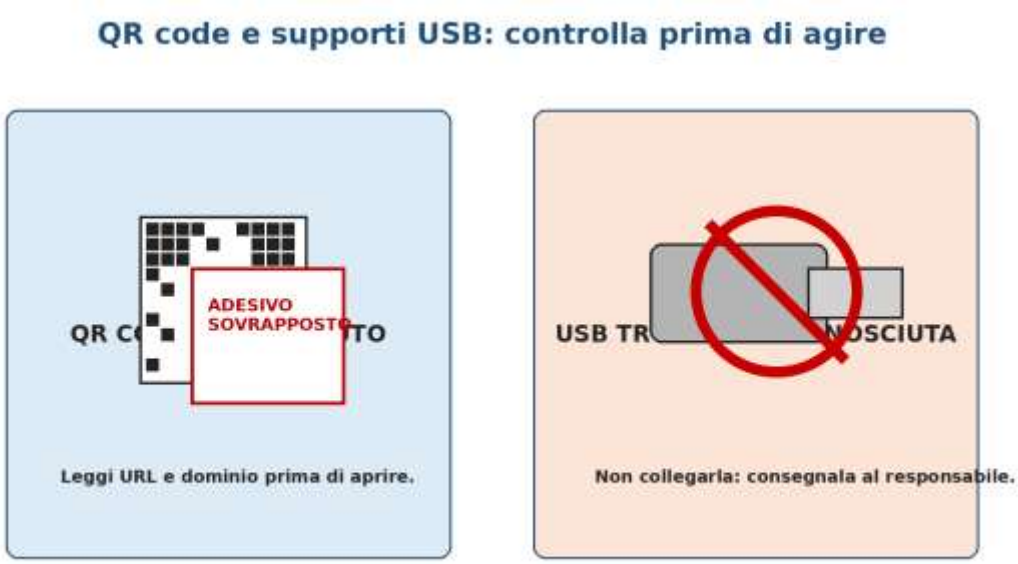

Figura 4 - QR code sospetti e supporti USB sconosciuti richiedono prudenza.

DA RICORDARE
Non collegare una chiavetta USB trovata o ricevuta da una persona sconosciuta. In azienda o a scuola consegnala al referente senza provarla. La curiosità è utile per imparare, ma non è una buona ragione per collegare dispositivi sconosciuti.

10. Il metodo FERMA

Quando una richiesta ti sembra strana, applica un metodo semplice: Fermati, Esamina, Ragiona, Mostra, Agisci. Il metodo verrà ripreso anche nella dispensa dedicata agli incidenti. L'idea fondamentale è rallentare prima di compiere un'azione difficile da annullare.

Lettera	Azione	Significato pratico
F	Fermati	non fare clic e non rispondere subito;
E	Esamina	controlla mittente, dominio, allegati, richiesta e urgenza;
R	Ragiona	chiediti se la richiesta è coerente e necessaria;
M	Mostra	fai vedere il messaggio a docente, tecnico o adulto competente;
A	Agisci	procedi solo dopo la verifica, oppure segnala e chiudi.

11. Reti Wi-Fi pubbliche e hotspot

Una rete Wi-Fi gratuita può essere utile, ma non deve essere considerata automaticamente sicura. Il nome della rete può essere imitato e non sempre è chiaro chi gestisca realmente il collegamento. Per attività delicate, come home banking, pagamenti o modifica di password, è preferibile usare una rete conosciuta oppure la connessione dati personale.

Figura 5 - Le reti Wi-Fi pubbliche richiedono prudenza.

12. Permessi delle app e notifiche del browser

Quando installi un'applicazione oppure visiti un sito, puoi ricevere richieste di autorizzazione: accesso alla fotocamera, al microfono, alla posizione, alle notifiche o ai file. Non accettare automaticamente. Chiediti se il permesso è coerente con lo scopo dell'app. Una calcolatrice che chiede accesso ai contatti oppure un sito casuale che vuole inviare notifiche meritano attenzione.

13. Truffe ricorrenti da riconoscere

Le tecniche cambiano, ma molti copioni si ripetono: finto pacco da sbloccare con un piccolo pagamento, multa urgente, rimborso fiscale, premio inatteso, falso supporto tecnico, richiesta di codice temporaneo, invito a installare un'app per ricevere assistenza. Il dettaglio cambia, ma l'obiettivo resta spingere la persona ad agire prima di ragionare.

14. Glossario essenziale

Termine	Significato
Malware	software progettato per causare danni, rubare informazioni o disturbare il funzionamento normale;
Virus	malware che si collega ad altri file e si attiva quando vengono eseguiti;
Worm	malware capace di propagarsi autonomamente attraverso reti e sistemi;
Trojan	programma apparentemente innocuo che nasconde funzioni dannose;
Ransomware	malware che cifra o blocca dati e sistemi;
Phishing	truffa tramite messaggi o siti imitati;
Smishing	phishing tramite SMS o messaggi sul telefono;
Vishing	inganno tramite telefonata o messaggio vocale;
Ingegneria sociale	tecnica che sfrutta fiducia, fretta, paura o curiosità della persona;
Dominio	nome principale di un sito Web.

15. Sintesi operativa

La sicurezza quotidiana nasce da una serie di piccole decisioni: aggiornare i programmi, non installare software da fonti incerte, controllare il dominio, non fidarsi della sola grafica, non comunicare codici temporanei, evitare chiavette sconosciute e chiedere aiuto quando la richiesta non è chiara. Un utente prudente non è quello che sa tutto, ma quello che si ferma prima di compiere un'azione rischiosa.

16. Domande di verifica

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

1. Che cosa significa sicurezza informatica?
2. Che cos'è un malware?
3. Qual è la differenza tra virus e worm?
4. Perché un trojan può essere difficile da riconoscere?
5. Che cosa fa un ransomware?
6. A che cosa servono gli aggiornamenti di sicurezza?
7. Perché un antivirus non basta da solo?
8. Che cos'è l'ingegneria sociale?
9. Quali emozioni vengono spesso sfruttate dagli attaccanti?
10. Che cos'è il phishing?
11. Che cos'è lo smishing?
12. Che cos'è il vishing?
13. Perché il logo di un'azienda non dimostra che un messaggio sia autentico?
14. Che cosa devi controllare prima di aprire un link?
15. Perché un risultato sponsorizzato richiede prudenza?
16. Che rischio può nascondere un QR code?
17. Che cosa devi fare se trovi una chiavetta USB?
18. Che cosa sono le USB dead drops?
19. Perché non devi comunicare un codice temporaneo?
20. Che cosa significa applicare il metodo FERMA?

17. Risposte ragionate

1. È l'insieme di regole, comportamenti e strumenti che proteggono persone, dati, dispositivi, account e reti.
2. È un programma o componente software progettato per danneggiare, spiare, rubare informazioni oppure disturbare il funzionamento normale.
3. Il virus si lega ad altri file e si attiva quando vengono eseguiti; il worm può propagarsi autonomamente attraverso reti e sistemi.
4. Perché può presentarsi come un programma apparentemente utile o innocuo.

5. Blocca o cifra file e sistemi e tenta di ottenere un riscatto.
6. Correggono errori e vulnerabilità che potrebbero essere sfruttati dagli attaccanti.
7. Perché nessun singolo strumento può prevenire tutti gli errori, gli inganni e le minacce possibili.
8. È una tecnica che sfrutta fiducia, paura, curiosità o fretta per convincere una persona a fare qualcosa di rischioso.
9. Fretta, paura, curiosità, desiderio di un premio, fiducia nell'autorità e segretezza.
10. È una truffa in cui un messaggio o un sito imitano un soggetto affidabile per ottenere dati o denaro.
11. È una forma di phishing che usa SMS o messaggi sul telefono.
12. È una forma di inganno che usa telefonate o messaggi vocali.
13. Perché logo, colori e grafica possono essere copiati facilmente.
14. Controlla mittente, indirizzo reale, dominio e coerenza della richiesta.
15. Perché l'evidenza grafica non garantisce che il risultato sia sicuro o ufficiale.
16. Può portare a un sito falso oppure avviare un download rischioso.
17. Non collegarla: consegnala al docente o al referente competente.
18. Sono supporti USB collocati in luoghi pubblici per lo scambio anonimo di file; non devono essere usati su dispositivi personali, scolastici o aziendali.
19. Perché può permettere a un attaccante di superare una protezione dell'account.
20. Significa fermarsi, esaminare, ragionare, mostrare a una persona competente e agire solo dopo la verifica.

18. Esercizi pratici e attività

Svolgi le attività con calma e senza usare messaggi reali contenenti dati personali. Quando lavori in laboratorio, segui sempre le indicazioni del docente.

1. Analizza tre email simulate preparate dal docente e individua i segnali di rischio.
2. Scrivi cinque esempi di oggetti email sospetti e spiega perché possono creare urgenza.
3. Confronta due domini simili e indica quale potrebbe essere quello ufficiale.
4. Crea una tabella con virus, worm, trojan, spyware e ransomware.
5. Descrivi il comportamento corretto davanti a un SMS relativo a un pacco inatteso.
6. Disegna un manifesto con un QR code e indica dove potrebbe essere sovrapposto un adesivo falso.
7. Prepara una checklist di cinque controlli prima di scaricare un programma.
8. Spiega che cosa faresti trovando una chiavetta USB vicino alla scuola.
9. Scrivi un dialogo breve tra un falso tecnico e un utente prudente.
10. Prepara un cartello con il metodo FERMA.
11. Elenca tre aggiornamenti importanti per un PC e tre per uno smartphone.
12. Spiega perché una finestra Web che invita a disattivare l'antivirus è sospetta.
13. Individua tre comportamenti che riducono il rischio di ransomware.
14. Crea una mini guida per un compagno più giovane: "Prima di cliccare, controlla".
15. Simula una segnalazione al docente di una email sospetta.

19. Checklist personale prima di cliccare

CHECKLIST FERMA
Il mittente è davvero quello atteso? Il dominio è corretto? La richiesta è coerente? Ci sono urgenza, paura o premio sospetto? Il link porta a un sito ufficiale? L'allegato era previsto? Sto per comunicare password, PIN o codice temporaneo? Ho chiesto aiuto se ho dubbi?