



Phishing e le sue varianti

Come riconoscere un inganno che arriva da e-mail, SMS, telefono e codici QR

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



Indice

Come usare questa dispensa 3

1. Un inganno che sembra vero 3

1.1 Perché funziona, anche con persone attente 5

1.2 Che cosa rischia davvero una segreteria 5

2. Le varianti: stesso obiettivo, canali diversi 6

2.1 Spear phishing: il messaggio fatto su misura 7

2.2 Smishing: l'esca arriva sul telefono 7

2.3 Vishing: la voce che sembra sicura 8

2.4 Quishing: il codice QR che nasconde il link 8

3. I segnali d'allarme 9

3.1 Caso pratico: la finta mail dell'Agenzia delle Entrate 10

4. La lista «fermati e controlla» 10

4.1 Il numero ufficiale: dove si trova davvero 12

4.2 Due regole che valgono per tutti 13

5. Tre casi dal lavoro di ogni giorno 13

5.1 Caso 1: la fattura che non aspettavi 14

5.2 Caso 2: il QR sull'avviso del parcheggio 14

5.3 Caso 3: il «tecnico» che chiama 15

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**
>
> Riconoscere il phishing e le sue varianti (spear phishing, smishing, vishing, quishing) e applicare ogni volta la lista «fermati e controlla» prima di cliccare, aprire o rispondere.

Che cosa saprai fare alla fine

- Spiegare che cos'è il phishing e perché funziona anche con persone attente.
- Distinguere phishing, spear phishing, smishing, vishing e quishing dal canale con cui arrivano.
- Riconoscere i segnali d'allarme di un messaggio sospetto.
- Applicare la lista «fermati e controlla»: mittente, fretta, link, allegato atteso.
- Verificare una richiesta dubbia chiamando il numero ufficiale dell'ente.

1. Un inganno che sembra vero

Il truffatore non ha bisogno di forzare il tuo computer, se riesce a convincerti ad aprirgli la porta.

È lunedì mattina nella segreteria dello Studio Esempio. Marta apre la posta e trova un messaggio che sembra del corriere: «Il suo pacco è bloccato, confermi i dati entro oggi». Aspettava davvero un pacco. Il logo è quello giusto, il tono è gentile ma deciso. Il dito è già sul link.



Un messaggio atteso può diventare un'esca.

Quel messaggio è **phishing**. La parola viene dall'inglese *fishing*, cioè «pescare»: il truffatore lancia un'esca e aspetta che qualcuno abbocchi. Finge di essere una persona o un ente di cui ti fidi (una banca, un corriere, l'Agenzia delle Entrate, un collega, il direttore) per convincerti a fare una di queste tre cose: cliccare un link, aprire un allegato, comunicare dati riservati.



Come funziona un attacco di phishing, dall'esca al furto

1.1 Perché funziona, anche con persone attente

Il phishing non attacca le macchine, attacca le persone. Non c'è nessuna falla da sfruttare nel computer: la falla è la fretta, la fiducia, la distrazione di un lunedì mattina. Per questo cade anche chi è competente.

I truffatori usano quasi sempre le stesse leve. Fanno leva sull'**urgenza** («entro oggi»), sulla **paura** («il suo conto sarà sospeso»), sull'**autorità** («sono il direttore»), sulla **curiosità** («una foto di te») o sul desiderio di essere **utili** («mi serve una mano»). Se un messaggio ti spinge ad agire senza pensare, è già un segnale.



Riconoscere la pressione aiuta a rallentare.

L'IDEA IN UNA RIGA

Il phishing cambia canale e travestimento, ma l'obiettivo è sempre lo stesso: farti agire prima di pensare.

1.2 Che cosa rischia davvero una segreteria

Se Marta inserisce la sua password su una pagina falsa, il truffatore può entrare nella posta dello studio, leggere i messaggi dei clienti, scaricare gli elenchi con nomi e codici fiscali e mandare altri messaggi a nome di Marta. Una sola password rubata apre la porta a tutto il resto. È il motivo per cui questa lezione viene subito dopo quella sul malware: molti attacchi cominciano proprio da un messaggio come questo.



Una password rubata può esporre la posta e i contatti.

2. Le varianti: stesso obiettivo, canali diversi

Quando le e-mail false sono diventate più facili da riconoscere, i truffatori non hanno smesso: hanno cambiato strada. Oggi lo stesso inganno può arrivare per posta elettronica, per SMS, per telefono o con un codice QR. Cambia il canale, non lo scopo.

Variante	Canale	Esempio
Phishing	E-mail	«Il suo conto è sospeso, acceda subito»
Spear phishing	E-mail mirata a una persona	Un falso messaggio del direttore alla segretaria: «Fai subito questo bonifico»
Smishing	SMS	«Pacco in giacenza, paghi 1,99 euro di spese»
Vishing	Telefonata	Un falso operatore della banca che chiede il codice ricevuto per SMS
Quishing	Codice QR	Un QR falso sul parchimetro o su un volantino che porta a un sito-trappola

Il phishing cambia canale, non obiettivo.



Cambia il canale, l'obiettivo rimane l'inganno.

2.1 Spear phishing: il messaggio fatto su misura

Spear vuol dire «fiocina»: non si getta una rete a caso, si prende di mira un pesce preciso. Il truffatore studia la vittima. Guarda il sito dello studio, i profili pubblici sui social, i nomi dei colleghi. Poi scrive un messaggio credibile, con il nome giusto e il tono giusto.

> **CASO PRATICO: IL BONIFICO DEL DIRETTORE**
>
> Alla segreteria di un piccolo ente arriva un messaggio che sembra del direttore, il dottor Rossi: «Sono in riunione, non posso telefonare. Devi fare subito un bonifico urgente a un nuovo fornitore, ti mando l'IBAN. Poi ti spiego».
>
> Il nome è giusto, il tono è quello del direttore. Ma l'indirizzo di posta non è quello dell'ente: è un indirizzo gratuito con un nome simile. E la richiesta ha tutti i segnali di una truffa: fretta, segretezza, soldi, nessuna possibilità di telefonare.
>
> **Che cosa fare:** non rispondere al messaggio. Chiamare il direttore sul numero che già conosci, oppure chiedere conferma di persona o a un collega. Per i pagamenti, una regola di studio semplice: nessun bonifico nuovo senza una seconda conferma su un altro canale.

2.2 Smishing: l'esca arriva sul telefono

Il nome unisce *SMS* e *phishing*. Il messaggio sembra del corriere, della banca, dell'ufficio postale, del gestore telefonico: «Pacco in giacenza, paghi 1,99 euro di spese di consegna».

La cifra è piccola apposta, così non ti insospettisce. Ma il link porta a una pagina che chiede i dati della carta di credito, e quei dati servono per ben altro che 1,99 euro.

Sul telefono è più difficile controllare l'indirizzo e si tende a fidarsi di più, perché l'SMS sembra una cosa personale. Vale lo stesso consiglio: non toccare il link, apri tu l'app o il sito ufficiale del corriere e controlla lì se c'è davvero un pacco.

2.3 Vishing: la voce che sembra sicura

Il *vishing* usa la voce (*voice* più *phishing*). Ti telefona qualcuno che si presenta come operatore della tua banca: «Abbiamo rilevato un movimento sospetto, per bloccarlo mi dica il codice che le arriva con un SMS». Il tono è professionale e rassicurante. Il codice, in realtà, serve al truffatore per autorizzare un'operazione a tuo nome.

> **REGOLA D'ORO**
>
> Una banca vera non ti chiede mai per telefono password, codici ricevuti per SMS o PIN. Se ti chiedono un codice, stai parlando con un truffatore. Riaggancia e richiama tu, dal numero scritto sul sito ufficiale o sulla tessera.

A volte il numero che compare sul display sembra quello giusto, perché i truffatori possono falsificarlo. Per questo non basta guardare chi chiama: conta cosa ti chiedono.

2.4 Quishing: il codice QR che nasconde il link

Un codice QR è un quadrato fatto di puntini che, inquadrato con la fotocamera, apre un indirizzo web. Il problema è che a occhio non puoi leggere dove porta. Un truffatore incolla un adesivo con un QR falso sul parchimetro, sul totem del parcheggio, su una locandina o su un volantino. Chi lo inquadra arriva a una pagina che imita quella vera e chiede la carta di credito.

Il QR può arrivare anche dentro un'e-mail o un PDF. Spesso è un modo per portare l'attacco sul telefono, dove i controlli sono minori. Prima di aprire l'indirizzo, guarda l'anteprima che il telefono mostra: se il dominio non è quello che ti aspetti, chiudi. Sugli adesivi, controlla che non siano incollati sopra altri.

3. I segnali d'allarme

Nessun segnale da solo prova che un messaggio sia falso, e nessun messaggio falso li ha tutti. Ma più ne trovi, più devi essere prudente. Ecco i principali, con quello che devi guardare.

Segnale	Che cosa guardare
Mittente strano	Leggi l'indirizzo, non solo il nome. Un nome può essere finto, l'indirizzo dice da dove arriva davvero. «Agenzia Entrate» scritto da un indirizzo gratuito o con un dominio strano è un campanello.
Fretta o minaccia	«Entro oggi», «ultimo avviso», «il conto sarà chiuso». Un ente serio ti dà il tempo di controllare.
Saluto generico	«Gentile cliente» invece del tuo nome. Non è decisivo, ma un ente che ti conosce di solito ti chiama per nome.
Link sospetto	Il testo del link dice una cosa, l'indirizzo vero un'altra. Passa il mouse sopra, senza cliccare, e guarda in basso.
Allegato inatteso	Una fattura che non aspettavi, un «documento scansionato» da un mittente sconosciuto. Gli allegati con estensione doppia (come .pdf.exe) sono un classico.
Richiesta di dati	Password, PIN, codici, numeri di carta: nessun ente serio li chiede per e-mail, SMS o telefono.
Errori e stranezze	Frasi goffe, logo sfocato, traduzioni strane. Utili, ma non decisivi: oggi molti messaggi falsi sono scritti benissimo.

I segnali più comuni di un messaggio sospetto.



Messaggio affidabile e messaggio sospetto a confronto

NON FIDARTI DEL «SEMBRA SCRITTO BENE»

Gli errori di grammatica un tempo tradivano i messaggi falsi. Oggi i truffatori possono usare programmi di traduzione e scrittura automatica, e i testi risultano curati. Un messaggio scritto bene non è per questo un messaggio vero: guarda mittente, link e richiesta.

3.1 Caso pratico: la finta mail dell'Agenzia delle Entrate

Arriva una mail con intestazione dell'Agenzia delle Entrate (l'ufficio italiano che si occupa delle tasse): «È stato rilevato un rimborso a suo favore. Clicchi qui per inserire i dati della carta». Il logo è giusto. Ma l'indirizzo del mittente è un dominio qualsiasi, il saluto è generico e la richiesta riguarda la carta di credito.

Un ente pubblico non ti chiede i dati della carta in questo modo e non ti manda a pagine esterne con un link in un messaggio. Se pensi che ci sia qualcosa di vero, accedi tu al sito ufficiale scrivendo l'indirizzo a mano, oppure chiami l'ufficio.

4. La lista «fermati e controlla»

Riconoscere tutti i trucchi è impossibile, perché cambiano di continuo. Un'abitudine invece si può imparare. Prima di cliccare, aprire o rispondere, fermati un momento e fai quattro controlli. Poi, se hai ancora un dubbio, un quinto gesto.



Mittente, pressione, link, allegati e verifica su altro canale.

1. **Chi è davvero il mittente?** Leggi l'indirizzo, non solo il nome. Sul telefono, tocca il nome per vedere l'indirizzo completo.
2. **Mi mette fretta o mi minaccia?** Se sì, rallenta di proposito. La fretta è l'arma del truffatore.
3. **Dove porta il link?** Passa il mouse sopra, senza cliccare, e leggi l'indirizzo che compare in basso. Sul telefono, tieni premuto il link per vedere l'anteprima.
4. **Me lo aspettavo?** Se ricevi un allegato o una richiesta che non aspettavi, il fatto che sembri vero non basta.
5. **Nel dubbio, verifica.** Chiama l'ente con il numero ufficiale oppure chiedi a chi si occupa di informatica.



Il testo visibile può nascondere una destinazione diversa.

4.1 Il numero ufficiale: dove si trova davvero

Il numero da chiamare non è quello scritto nel messaggio sospetto: sarebbe come chiedere al truffatore se è un truffatore. Cercalo da una fonte tua: il sito dell'ente scritto a mano nella barra degli indirizzi, la bolletta, il contratto, la tessera della banca, l'estratto conto.



Richiama usando un recapito ottenuto da una fonte indipendente.

4.2 Due regole che valgono per tutti

- **Nessun pagamento nuovo o cambio di IBAN senza una seconda conferma** su un canale diverso da quello della richiesta, per esempio una telefonata a un numero già noto.
- **Nessuna password, nessun codice** si comunica a nessuno. Neanche a un collega, neanche al «tecnico». Un tecnico vero non ne ha bisogno.
- **In caso di dubbio, mostralo a qualcuno.** Una seconda persona guarda con occhi diversi e non ha la fretta addosso.



Un nuovo bonifico o cambio di IBAN richiede una conferma indipendente.

IN PAROLE SEMPLICI

Fermarsi non è perdere tempo. È l'unico gesto che i truffatori non possono sfruttare.

5. Tre casi dal lavoro di ogni giorno

Mettiamo in pratica quanto visto. Per ogni caso prova prima a decidere da solo che cosa faresti, poi leggi la risposta.

5.1 Caso 1: la fattura che non aspettavi

In una scuola arriva una mail: «In allegato la fattura scaduta, la preghiamo di saldare». Il mittente è sconosciuto, l'allegato si chiama *fattura.pdf.exe*. La segretaria non ha ordinato nulla a quel fornitore.

Cosa fare: non aprire l'allegato. Il nome con doppia estensione indica un programma che finge di essere un documento: può essere un malware, come hai visto nella lezione precedente. Controllare nell'archivio ordini se esiste davvero quel fornitore, avvisare il referente informatico e cancellare il messaggio.



Un allegato inatteso non diventa sicuro perché sembra una fattura.

5.2 Caso 2: il QR sull'avviso del parcheggio

Fuori dal negozio c'è un avviso: «Pagamento sosta, inquadra il QR». Sembra incollato un po' storto, sopra l'avviso originale. Il QR apre un sito con un modulo per pagare con carta.

Cosa fare: non inquadrarlo. Se il parcheggio ha un'app ufficiale o un parchimetro, usa quelli. Un adesivo incollato sopra l'avviso è un segnale d'allarme. Se hai già inserito la carta, chiama subito la banca per bloccarla e passa alla lezione dedicata a che cosa fare se succede.

5.3 Caso 3: il «tecnico» che chiama

Squilla il telefono: «Buongiorno, sono dell'assistenza del suo gestore di posta. Abbiamo notato un accesso anomalo, mi serve il codice che sta per arrivarle sul telefono per bloccarlo». Il tono è cortese e sicuro, e il codice arriva davvero mentre parlate.

Cosa fare: chiudere la telefonata. Il codice che arriva è proprio quello che serve al truffatore, che in quel momento sta provando ad entrare nel tuo account. Nessun servizio serio ti chiede quel codice a voce. Poi avvisa il referente informatico e cambia la password dal sito vero, come vedrai nelle lezioni successive.



Un codice appena arrivato non va comunicato a chi telefona.

SE HAI GIÀ CLICCATO

Non vergognarti e non nasconderlo: la rapidità conta più dell'imbarazzo. Isola il computer, avvisa subito il responsabile e cambia le password dal sito vero. I quattro passi completi sono nella lezione «Che cosa fare se succede».



Hai cliccato? Avvisa subito. Per esercitarti osserva senza aprire link o allegati.

Esercitazione pratica

Una breve esercitazione, da fare da solo o in coppia, con le ultime mail e i messaggi che hai ricevuto davvero.

1. Apri la cartella della posta indesiderata (spam) e scegli tre messaggi. Se non ne hai, usa quelli di una mail che ti pare strana degli ultimi giorni.
2. Per ciascuno scrivi su un foglio: chi è il mittente (indirizzo completo), che cosa chiede, quale leva usa (fretta, paura, autorità, curiosità).
3. Passa il mouse sopra ogni link, senza cliccare, e annota l'indirizzo che compare in basso: coincide con quello che il testo dichiara?
4. Applica la lista «fermati e controlla» e decidi per ognuno: cancello, segnalo o verifico con il numero ufficiale.
5. Se lavori in coppia, scambiatevi i fogli e discutete le differenze. Poi scrivete insieme la regola di studio per i bonifici nuovi.

AUTOVALUTAZIONE

Che differenza c'è tra phishing e spear phishing?

Perché una banca vera non ti chiede mai un codice per telefono?

Quali sono i quattro controlli della lista «fermati e controlla»?

Dove trovi il numero ufficiale da chiamare nel dubbio?

Le domande che arrivano in aula

Posso riconoscere il phishing dagli errori di grammatica?

Non più. Un tempo era un buon indizio, ma oggi molti messaggi falsi sono scritti con cura. Fidati meno del tono e più dei fatti: mittente, link, richiesta di dati o di soldi.

Se passo il mouse sul link e sembra normale, posso cliccare?

Se l'indirizzo coincide con quello che ti aspetti, è un buon segno, ma non è una garanzia. Se hai dubbi sul messaggio, non cliccare comunque: apri il sito scrivendo l'indirizzo a mano o dall'app ufficiale.

Ho cliccato un link sospetto ma non ho inserito niente. Sono a rischio?

Di solito il rischio principale è nell'inserire dati o scaricare qualcosa. Chiudi la pagina, non scaricare nulla e avvisa il referente informatico. Se hai scaricato o aperto un file, o inserito dati, passa subito ai passi della lezione dedicata.

Il messaggio sembra arrivare da un collega che conosco. Posso fidarmi?

Non sempre: l'indirizzo può essere falsificato o l'account del collega può essere stato rubato. Se la richiesta è insolita (soldi, password, file riservati), conferma con una telefonata o di persona.

Posso inquadrare un codice QR senza rischi?

Inquadrare di per sé non basta a farti del male, ma ti porta a una pagina che non conosci. Guarda l'indirizzo nell'anteprima prima di aprirla e non inserire mai password o dati di carta in una pagina raggiunta così, se non sei sicuro.

Come segnalo un tentativo di phishing?

Avvisa il referente informatico del tuo studio o della tua scuola. Se ci sono soldi o dati di terzi di mezzo, conserva i messaggi e rivolgiti alla Polizia Postale e delle Comunicazioni (il servizio della polizia che si occupa dei reati online), tramite commissariatodips.it.

Glossario

Termine	Che cosa significa
Codice QR	Quadrato di puntini che la fotocamera legge e traduce in un indirizzo web o in un testo.
IBAN	Il codice che identifica un conto corrente e a cui si indirizza un bonifico.

Termine	Che cosa significa
Mittente	Chi invia il messaggio; il vero indirizzo conta più del nome visualizzato.
Phishing	Inganno in cui un truffatore finge di essere un ente o una persona fidata per farti cliccare, aprire un allegato o dare dati riservati.
Quishing	Phishing tramite codice QR falso, per esempio su un adesivo o un volantino.
Smishing	Phishing via SMS, spesso con finti avvisi di corrieri o banche.
Spear phishing	Phishing mirato: il messaggio è costruito su misura per una persona precisa, usando informazioni che la riguardano.
Vishing	Phishing per telefono: chi chiama finge di essere, per esempio, un operatore della banca.

Per approfondire

Polizia Postale e delle Comunicazioni, Commissariato di P.S. online - commissariatodips.it, per segnalazioni e consigli sulle truffe online

Agenzia per la cybersicurezza nazionale (ACN) e CSIRT Italia - avvisi e guide sulle minacce informatiche in Italia

Garante per la protezione dei dati personali - garanteprivacy.it, schede informative su phishing e sicurezza dei dati

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. Gli esempi, i nomi e i domini (come ente-esempio.it) sono di fantasia. Le tecniche cambiano in fretta: conta più il criterio di controllo che i singoli esempi. Per qualsiasi segnalazione fai riferimento ai canali ufficiali indicati.