

Siti trappola e inganni

Indirizzi quasi uguali, telefonate convincenti e identità rubate: come difendersi dall'inganno

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



Indice

Come usare questa dispensa 3

1. Il sito che sembra quello giusto 3

1.1 Che cosa sono un dominio e un nome a dominio 4

1.2 Cybersquatting e typosquatting 4

2. Leggere un indirizzo senza farsi ingannare 5

2.1 La regola per trovare il dominio vero 7

2.2 Caratteri che si somigliano 7

2.3 I link accorciati 8

3. Come controllare e come difendersi 8

3.1 Cinque abitudini che salvano la giornata 9

3.2 Un negozio online sconosciuto: come capire se è serio 10

4. L'ingegneria sociale: manipolare le persone 11

4.1 Le leve che usa 12

4.2 Alcune tecniche, con esempi 13

4.3 Una procedura batte la buona volontà 14

5. Il furto di identità 14

5.1 Da dove arrivano i dati 14

5.2 Come ridurre il rischio 15

5.3 Se pensi di essere stato colpito 16

Esercitazione pratica 18

Le domande che arrivano in aula 19

Glossario 19

Per approfondire 20

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 un sito-trappola leggendo il dominio, difendersi con preferiti e controlli, e capire come l'ingegneria sociale e il furto di identità sfruttano le persone più delle macchine.

Che cosa saprai fare alla fine

- Spiegare che cosa sono cybersquatting e typosquatting.
- Leggere un indirizzo web e individuare il vero dominio.
- Controllare un sito prima di inserire password o dati di pagamento.
- Riconoscere le leve dell'ingegneria sociale e rispondere con una procedura.
- Ridurre il rischio di furto di identità e sapere come reagire.

1. Il sito che sembra quello giusto

Un solo carattere sbagliato in un indirizzo può portarti in una pagina identica a quella vera, ma gestita da un'altra persona.

Giulia lavora nella segreteria di un ente. Deve accedere al portale dei servizi, che ha l'indirizzo www.ente-esempio.it. Va di fretta, scrive l'indirizzo a memoria e preme invio. Compare una pagina identica: stesso logo, stessi colori, stessa casella per la password. Inserisce le credenziali. Poi si accorge che l'indirizzo era www.ente-esenpio.it, con una «n» al posto della «m».

Quella pagina era un sito-trappola. Chi l'ha costruito non ha violato nulla: ha semplicemente registrato un nome quasi uguale e ha aspettato che qualcuno sbagliasse a scrivere.



L'aspetto di una pagina può essere copiato: controlla l'indirizzo.

1.1 Che cosa sono un dominio e un nome a dominio

Il **nome a dominio** è la parte dell'indirizzo che identifica un sito, per esempio *ente-esempio.it*. Si registra presso società autorizzate e chiunque può registrare un nome libero, finché non è già preso. Non esiste un controllo che verifichi se il nome somiglia a quello di qualcun altro.

1.2 Cybersquatting e typosquatting

Il **cybersquatting** consiste nel registrare un nome a dominio uguale o molto simile al nome di un'azienda, di un ente o di una persona nota, per rivenderlo a caro prezzo o per sfruttarne la notorietà. Il termine viene dall'inglese *to squat*, «occupare abusivamente».

Il **typosquatting** ne è una variante: si registrano domini con errori di battitura probabili (*typo* significa «refuso»), sperando che l'utente sbagli a scrivere. Non serve ingannare nessuno con una mail: basta aspettare.

Sito vero	Esempi di sito-trappola
www.ente-esempio.it	www.ente-esempio.com (altra estensione)
www.ente-esempio.it	www.ente-esempIo.it (la «i» sostituita dal numero uno)
www.ente-esempio.it	www.ente-esempio-it.net (il punto diventa un trattino)
www.ente-esempio.it	www.ente-esenpio.it (una lettera cambiata)

Domini simili che ingannano l'occhio (esempi di fantasia).



Nomi simili ed errori di battitura possono essere sfruttati per ingannare.

Che cosa ospitano questi siti? Pagine che imitano quelle vere per **rubare credenziali**, negozi che vendono prodotti contraffatti o mai spediti, a volte pagine che diffondono **malware**, il software dannoso della lezione sul ransomware.

> **L'IDEA IN UNA RIGA**
>
> Il sito-trappola non ti attacca: aspetta che sbagli tu, oppure ti manda un link che sembra giusto.

2. Leggere un indirizzo senza farsi ingannare

Per riconoscere un indirizzo falso devi sapere come è fatto uno vero. Prendiamone uno di fantasia: **https://portale.ente-esempio.it/accesso**. Si legge a pezzi.



Le parti di un indirizzo web

- **https://** è il protocollo: indica che la connessione è cifrata, cioè i dati in viaggio sono resi illeggibili a chi li intercetta;
- **portale** è il sottodominio, una sezione scelta da chi gestisce il sito (può essere qualunque parola);
- **ente-esempio.it** è il dominio vero, la parte che conta, formata dal nome e dall'estensione (.it, .com, .net...);
- **/accesso** è il percorso, cioè la pagina dentro il sito.



Protocollo, sottodominio, dominio e percorso hanno funzioni diverse.

2.1 La regola per trovare il dominio vero

Cerca la prima barra (/) dopo https:// e guarda **le due parole che stanno subito prima, separate da un punto**. Quelle sono il dominio vero. Tutto ciò che sta più a sinistra può essere scelto liberamente da chi possiede il dominio.

> **IL TRUCCO DEL SOTTODOMINIO**
>
> Guarda questo indirizzo: **https://ente-esempio.it.accesso-sicuro.net/login**
>
> A prima vista sembra dell'ente, perché «ente-esempio.it» compare per primo. Ma il dominio vero è **accesso-sicuro.net**: tutto ciò che viene prima è solo un sottodominio scelto dal truffatore.
>
> Confronta con **https://servizi.ente-esempio.it/login**: qui il dominio vero è ente-esempio.it e «servizi» è un sottodominio dell'ente. Questo indirizzo è affidabile.



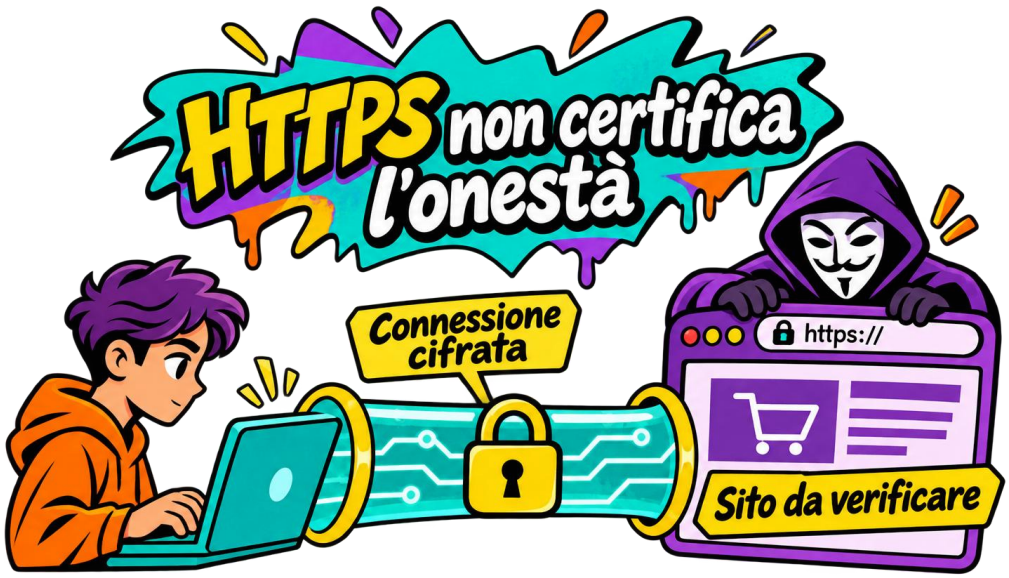
Il nome dell'ente all'inizio non prova che il sito gli appartenga.

2.2 Caratteri che si somigliano

Alcuni caratteri si confondono facilmente a occhio. Il numero zero e la lettera «o». Il numero uno e la lettera «l» minuscola. Due lettere affiancate, come «r» e «n», che somigliano a una «m». In alcuni casi i truffatori usano anche lettere di altri alfabeti, che sembrano identiche alle nostre. Il browser, il programma con cui navighi, a volte mostra questi indirizzi in una forma diversa proprio per segnalarlo, ma non puoi contarci.

IL LUCCHETTO NON VUOL DIRE «SITO ONESTO»

Il lucchetto accanto all'indirizzo (in Chrome, l'icona delle impostazioni a sinistra dell'indirizzo) indica solo che la connessione è cifrata. Anche un sito-trappola può averlo. Dice che nessuno spia i dati mentre viaggiano, non che il sito sia quello che dice di essere.



HTTPS protegge la connessione; non certifica l'onestà del sito.

2.3 I link accorciati

A volte il link è «accorciato» da un servizio apposito e non si vede dove porta. È comodo, ma in un messaggio inatteso è un motivo in più di sospetto. Meglio non aprirlo: vai tu direttamente sul sito ufficiale.

3. Come controllare e come difendersi

Le difese sono poche e semplici. Il difficile è trasformarle in abitudine, soprattutto quando si lavora di fretta.



Cinque abitudini per non cadere nel sito-trappola

3.1 Cinque abitudini che salvano la giornata

1. **Scrivi con attenzione** gli indirizzi che digiti a mano e rileggili prima di premere invio.
2. **Salva tra i preferiti** i siti importanti (banca, posta, portali dell'ente): ci arrivi con un clic, senza il rischio di un errore di battitura.
3. **Controlla sempre il dominio** nella barra degli indirizzi prima di inserire una password: leggi dall'estensione verso sinistra.
4. **Non seguire i link dei messaggi inattesi**: apri il sito dai preferiti o digitando l'indirizzo.
5. **Diffida degli annunci in cima ai risultati di ricerca**: possono essere sponsorizzati. Prima di cliccare, controlla che l'indirizzo mostrato sia quello giusto.



Rileggi, usa i preferiti e controlla prima di inserire credenziali.

Un aiuto in più: un gestore di password (lo vedrai nella lezione dedicata alle password) propone di solito le credenziali solo sul sito per cui le hai salvate. Se non le propone, può voler dire che ti trovi su un sito diverso da quello vero. Non è infallibile, ma è un buon campanello.

3.2 Un negozio online sconosciuto: come capire se è serio

I siti-trappola non servono solo a rubare password. Molti sono negozi falsi, con prezzi che sembrano un affare. Prima di comprare da un sito che non conosci, guarda alcuni segnali.

Segnale	Che cosa può voler dire
Prezzi molto più bassi di tutti gli altri	Un'offerta troppo bella per essere vera spesso lo è.
Nessun dato dell'azienda (nome, indirizzo, partita IVA)	Un negozio serio li mostra e li puoi verificare.
Solo pagamenti che non puoi annullare (bonifico, ricarica)	Se qualcosa va storto, non puoi tornare indietro.
Recensioni tutte uguali e tutte entusiaste	Possono essere state scritte da una persona sola.
Indirizzo strano o con estensione insolita	Controlla da quanto esiste e che cosa dicono altri su di lui.

Segnali che fanno sospettare un negozio online falso.



Indizi da verificare prima di comprare.

CASO PRATICO: I TONER A METÀ PREZZO

La segreteria di un piccolo studio cerca toner per la stampante e trova un sito con i prezzi dimezzati. L'indirizzo è molto simile a quello di un grosso rivenditore noto, con un trattino in più.

Il sito non mostra nessuna ragione sociale, accetta solo bonifico e promette sconti «solo per oggi».

Che cosa fare: non pagare. Aprire il sito del rivenditore noto dai preferiti, confrontare, e segnalare l'indirizzo sospetto al referente informatico.

4. L'ingegneria sociale: manipolare le persone

Forzare un computer è difficile. Convincere una persona gentile a dare la password, molto più facile.

L'**ingegneria sociale** è l'arte di manipolare le persone, più che le macchine, per ottenere informazioni o accessi. Il phishing che hai visto nella lezione precedente ne è una forma. Ma l'ingegneria sociale è più ampia: può essere una telefonata, un cartellino falso, una persona in giacca e cravatta che entra dietro di te.

4.1 Le leve che usa

Cambiano le storie, non le leve. Chi ti inganna cerca di toccare uno di questi punti sensibili.



Le cinque leve dell'ingegneria sociale

Leva	Come suona	Che cosa fare
Autorità	«Sono il direttore» o «sono della polizia»	Verifica con un numero che conosci già.
Urgenza	«Serve subito, è un'emergenza»	Rallenta: l'urgenza è fatta per non farti pensare.
Paura	«Il suo account sarà chiuso»	Controlla dal sito vero, non dal messaggio.
Aiuto e simpatia	«Mi dai una mano? Non trovo la password»	Essere gentili non vuol dire dare accessi.
Curiosità	Una chiavetta trovata, un file «riservato»	Non è tuo e non sai che cosa contiene.

Le cinque leve più usate dall'ingegneria sociale.



Autorità, urgenza, paura, aiuto e curiosità possono diventare leve d'inganno.

4.2 Alcune tecniche, con esempi

- **Pretesto (pretexting):** il truffatore si inventa una storia credibile. Esempio: telefona fingendosi dell'assistenza tecnica per farsi dare la password.
- **Esca (baiting):** lascia un oggetto allettante. Esempio: una chiavetta USB con scritto «Stipendi» lasciata nel parcheggio. Chi la inserisce nel computer può installare un malware.
- **Accesso fisico (tailgating):** si infila dietro di te in un ufficio, magari con le mani piene di scatole, e tu gli tieni la porta.
- **Raccolta di informazioni:** prima di attaccare, il truffatore guarda organigrammi, social e siti per sapere chi sei e con chi lavori.

> **CASO PRATICO: IL FINTO TECNICO**
>
> Telefona un uomo cortese: «Sono dell'assistenza informatica, stiamo aggiornando i computer dell'ente. Mi serve la sua password per finire in fretta; altrimenti rischiamo di bloccarle la posta».
>
> Sa il nome della collega e quello del responsabile, il che lo rende credibile. Ma chiede la password, il segno di un truffatore: un vero tecnico non ne ha bisogno.
>
> **Che cosa fare:** rifiutare con gentilezza, chiedere nome e numero, riagganciare e chiamare il referente informatico al numero di sempre. Poi segnalare il tentativo, perché lo stesso signore potrebbe telefonare a un'altra collega.



Un nome conosciuto non autorizza la richiesta della tua password.

4.3 Una procedura batte la buona volontà

Dire di no a una persona gentile che dice di aver bisogno di aiuto è difficile. Per questo serve una regola scritta, valida per tutti, anche per il direttore: così il «no» non è personale ma è la procedura. Per esempio: **nessuna password si comunica a nessuno**; **ogni visitatore ha un accompagnatore**; **ogni richiesta strana si verifica su un altro canale**.

5. Il furto di identità

Il **furto di identità** consiste nell'usare i dati di qualcuno per aprire conti, fare acquisti, firmare contratti o chiedere finanziamenti a suo nome. Chi lo subisce può accorgersene mesi dopo, quando arriva una richiesta di pagamento per qualcosa che non ha mai comprato.

5.1 Da dove arrivano i dati

I dati possono arrivare da molte strade, e molte le hai già incontrate in queste lezioni: una password rubata con il phishing, un sito-trappola, una violazione di dati di un servizio, un documento lasciato in vista, un profilo pubblico sui social pieno di informazioni (data di nascita, città, nome degli animali, luoghi frequentati).

Messi insieme, questi frammenti dicono molto. Per un truffatore, nome, data di nascita e indirizzo sono già un buon inizio per sembrare credibile al telefono o per indovinare una risposta di sicurezza.



I dati sottratti possono essere usati per impersonare una persona.

5.2 Come ridurre il rischio

- **Condividi il minimo.** Non pubblicare sui social documenti, codice fiscale, foto di biglietti, carte o tessere.
- **Non lasciare documenti in giro.** Fotocopie di carte d'identità e tessere non vanno lasciate sulla scrivania o nella stampante.
- **Controlla le tue password e i tuoi account.** Una password riutilizzata su più servizi apre tutte le porte quando uno viene violato (ne parliamo nella lezione dedicata).
- **Guarda gli estratti conto.** Un addebito sconosciuto va chiesto subito alla banca.
- **Distruggi i documenti prima di buttarli.** Un foglio con dati personali non va nel cestino così com'è.



Condividi il minimo e custodisci anche i documenti degli altri.

DOCUMENTI DI TERZI

In una segreteria passano carte d'identità, codici fiscali, documenti di iscritti e clienti. Il furto di identità può colpire anche loro, e tu rispondi di come li custodisci. Se ne perdi uno, avvisa subito il responsabile (ne parliamo nella lezione su privacy e protezione dei dati).

5.3 Se pensi di essere stato colpito

Se scopri che qualcuno usa i tuoi dati o quelli di un cliente, non aspettare. Avvisa la banca se ci sono pagamenti, cambia le password degli account interessati, conserva le prove e rivolgiti alla Polizia Postale e delle Comunicazioni (commissariatodips.it). I passi completi sono nella lezione «Che cosa fare se succede».



Avvisa, proteggi gli accessi, conserva le prove e contatta le autorità.

Esercitazione pratica

Una breve esercitazione con il browser che usi ogni giorno, senza installare nulla.

1. Apri il browser e scrivi a mano l'indirizzo di un sito che usi spesso (la banca, la posta, il portale dell'ente). Controlla che sia quello giusto e salvalo tra i preferiti.
2. Prendi quattro indirizzi di fantasia e per ciascuno scrivi qual è il dominio vero: https:*servizi.ente-esempio.it/login, https:*ente-esempio.it.accesso-sicuro.net/login, https:*www.ente-esemp1o.it, https:*ente-esempio-it.net/accesso.
3. Cerca sul motore di ricerca il nome della tua banca o di un ente. Guarda se il primo risultato è un annuncio e confronta l'indirizzo con quello dei preferiti.
4. Scrivi su un foglio la procedura di studio per le telefonate sospette: che cosa si risponde, chi si chiama, dove si segnala.
5. Fai l'inventario di che cosa si sa di te in pubblico, sui social: data di nascita, luogo di lavoro, nomi di familiari. Che cosa toglieresti?

AUTOVALUTAZIONE

Perché www.ente-esemp1o.it è un pericolo?

Qual è il dominio vero di https://ente-esempio.it.accesso-sicuro.net/login?

Che differenza c'è tra cybersquatting e typosquatting?

Che cosa fai se un «tecnico» ti telefona e ti chiede la password?

Le domande che arrivano in aula

Se il sito ha il lucchetto, è sicuro?

Non necessariamente. Il lucchetto dice che la connessione è cifrata, non che il sito sia onesto. Anche un sito-trappola può averlo: controlla sempre il dominio.

Basta scrivere l'indirizzo a mano per essere al sicuro?

Riduce il rischio, ma un errore di battitura può portarti proprio su un sito-trappola. Per i siti importanti, i preferiti sono più sicuri che digitare ogni volta.

Come faccio a sapere se un negozio online è affidabile?

Guarda i dati dell'azienda (nome, indirizzo, partita IVA), le modalità di pagamento, i prezzi troppo bassi e cerca opinioni fuori dal sito. Se hai dubbi, paga con un metodo che permette di contestare l'addebito, non con un bonifico.

Come mi comporto con chi mi chiede aiuto e sembra in buona fede?

Con gentilezza, ma seguendo la procedura. Un vero collega capisce una verifica: «Ti richiamo io su un numero che conosco» non offende nessuno.

Posso sapere se i miei dati sono già in circolazione?

Esistono servizi che avvisano se un indirizzo e-mail compare in una violazione nota. Non danno una garanzia completa, e conviene usare solo servizi affidabili e ufficiali. In ogni caso: password diverse per ogni servizio.

Si può registrare un dominio simile al mio per proteggersi?

Sì, molte organizzazioni registrano le varianti più probabili, come l'estensione .com o l'errore di battitura più comune. Non protegge da tutto, ma riduce il rischio. Chi ha un marchio può anche avviare procedure per riavere un dominio registrato in malafede, con l'aiuto di un legale.

Glossario

Termine	Che cosa significa
Browser	Il programma con cui si navigano i siti web.
Cybersquatting	Registrare un nome a dominio uguale o simile a quello di un'azienda o di una persona nota, per rivenderlo o sfruttarne la notorietà.
Furto di identità	Uso dei dati di qualcuno per aprire conti, fare acquisti o firmare contratti a suo nome.

Termine	Che cosa significa
Ingegneria sociale	Manipolare le persone, più che le macchine, per ottenere informazioni o accessi.
Malware	Software dannoso creato per danneggiare un computer o rubare dati.
Nome a dominio	La parte dell'indirizzo che identifica un sito, per esempio ente-esempio.it.
Sottodominio	Parte dell'indirizzo che sta a sinistra del dominio vero e che il gestore sceglie liberamente.
Typosquatting	Registrare domini con errori di battitura probabili, sperando che l'utente sbagli a scrivere.

Per approfondire

Registro .it - il registro dei nomi a dominio italiani, con regole e informazioni sulla registrazione

Polizia Postale e delle Comunicazioni - commissariatodips.it, per segnalazioni e consigli su truffe e furti di identità online

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

Garante per la protezione dei dati personali - garanteprivacy.it, indicazioni su furto di identità e tutela dei dati

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. Gli esempi, i nomi e i domini (come ente-esempio.it) sono di fantasia. Le regole di registrazione dei domini e le procedure di segnalazione possono cambiare: controlla sempre i canali ufficiali indicati.