



Introduzione al corso

A chi serve, che cosa imparerai e come seguirlo

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



Indice

Come usare questa dispensa....3

1. Perché questo corso....3

2. A chi è rivolto e che cosa serve....4

2.1 Che cosa serve....5

3. Che cosa imparerai....5

4. Il programma, lezione per lezione....5

4.1 Le minacce, in breve....6

4.2 Le difese, in breve....8

4.3 Se succede....10

5. Come seguire il corso....11

6. Chi te lo racconta....12

Preparazione....13

Le domande che arrivano in aula....14

Glossario....14

Per approfondire....14

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**
>
> Capire se il corso fa per te, sapere che cosa contiene ogni lezione e in che ordine seguirle, e preparare gli strumenti per cominciare.

Che cosa saprai fare alla fine

- Sapere a chi è rivolto il corso e che cosa serve per seguirlo.
- Conoscere il programma, lezione per lezione.
- Scegliere un modo di studiare adatto a te.
- Preparare la cartella di lavoro e gli strumenti per le esercitazioni.

1. Perché questo corso

Lunedì mattina, in segreteria, arriva una mail del direttore: «Fai subito questo bonifico, ti spiego dopo». Che cosa fai?

È una situazione che capita davvero, ed è una truffa che ha un nome: spear phishing. Chi la riconosce in tempo evita un danno. Chi non la riconosce paga, a volte con i soldi, a volte con i dati degli altri.



Una richiesta urgente merita attenzione.

Il computer di un ufficio contiene nomi, indirizzi, codici fiscali, a volte documenti sanitari o economici di molte persone. Proteggerli è un obbligo di legge, ma prima ancora è una questione di **fiducia**: chi ti ha affidato i suoi dati si aspetta che tu li tratti con cura.

> **L'IDEA IN UNA RIGA**
>
> Quasi tutti gli incidenti nascono da un errore umano: per questo la difesa migliore sei tu, e si impara.

2. A chi è rivolto e che cosa serve

Il corso parte da zero. Non servono competenze tecniche: bastano la curiosità e l'abitudine a usare il computer, la posta elettronica e il telefono. È pensato per chi lavora in una segreteria, in uno studio, in una scuola, in un piccolo negozio, ma vale anche a casa.

È per te se	Forse non fa per te se
Usi ogni giorno computer, posta e telefono per lavoro	Sei già un tecnico della sicurezza e cerchi i dettagli di un attacco
Gestisci dati di clienti, iscritti, colleghi	Cerchi un corso su come difendere una grande rete aziendale

È per te se	Forse non fa per te se
Vuoi capire che cosa fare, senza paroloni	Non usi mai strumenti digitali

A chi serve il corso.

2.1 Che cosa serve

- un computer con **Windows 11** (gli esempi usano quello);
- una casella di posta elettronica e un telefono;
- una cartella sul computer in cui salvare i tuoi appunti;
- carta e penna per le esercitazioni.

> **ATTENZIONE**
>
> Nelle esercitazioni usa sempre dati inventati o tuoi. Non usare mai dati di clienti, colleghi o iscritti veri per provare.

3. Che cosa imparerai

Alla fine del corso saprai fare queste cose, e non sono teoria: le userai già dal giorno dopo.

- **Riconoscere** malware, ransomware, phishing e siti trappola prima di cadere nell'inganno;
- **Scegliere** password solide e attivare la verifica in due passaggi;
- **Proteggere** il computer con aggiornamenti, Sicurezza di Windows, blocco dello schermo e cifratura;
- **Organizzare** copie di sicurezza che funzionano davvero, con la regola 3-2-1;
- **Trattare** i dati personali come richiede la legge, dalla copia nascosta alla notifica di una violazione;
- **Reagire** nel modo giusto quando succede qualcosa.

4. Il programma, lezione per lezione

Le lezioni sono nove e vanno seguite in ordine. Le prime quattro spiegano **da che cosa** ci difendiamo, le successive quattro **come** ci difendiamo, l'ultima **che cosa fare** quando le difese non bastano.

Lezione	Titolo	Che cosa saprai fare dopo
1	Che cos'è la sicurezza informatica	Spiegare che cosa si protegge e perché l'errore umano è il rischio principale
2	Malware e ransomware	Riconoscere i tipi di software dannoso e sapere perché non si paga il riscatto
3	Phishing e le sue varianti	Smascherare e-mail, SMS, telefonate e codici QR truffa
4	Siti trappola e inganni	Controllare un indirizzo web e riconoscere l'ingegneria sociale
5	Password e verifica in due passaggi	Creare password solide e attivare il secondo controllo
6	Proteggere dispositivi e reti	Mettere in sicurezza il computer, le chiavette e il Wi-Fi
7	Il backup e la regola 3-2-1	Organizzare copie di sicurezza e provare il ripristino
8	Privacy e protezione dei dati	Applicare le buone prassi sui dati personali e gestire una violazione
9	Che cosa fare se succede	Seguire i passi giusti in caso di incidente

Il programma del corso.

4.1 Le minacce, in breve

Le prime quattro lezioni servono a riconoscere il nemico. Si parte dal software dannoso: il **ransomware** blocca i tuoi file e chiede un riscatto per restituirli.



Il ransomware blocca i file e chiede un riscatto.

Poi vengono gli inganni che arrivano da fuori: il **phishing** non passa solo dalle mail, ma anche da messaggi, telefonate e codici QR.



Il phishing può arrivare attraverso canali diversi.

Infine i siti trappola e l'ingegneria sociale, cioè gli inganni che puntano sulle persone più che sulle macchine.



Gli inganni fanno leva sulle persone.

4.2 Le difese, in breve

Le quattro lezioni successive insegnano a difendersi. Per gli accessi servono due difese complementari: password solide e verifica in due passaggi.



Proteggi gli accessi con password solide e verifica in due passaggi.

Poi si passa agli strumenti di ogni giorno: il computer, le chiavette e il Wi-Fi vanno protetti con poche regole chiare.



La sicurezza riguarda anche gli strumenti che usi ogni giorno.

Il backup segue la regola 3-2-1, per avere sempre copie che funzionano quando servono.



Regola 3-2-1: copie diverse, disponibili quando servono.

Infine la privacy: i dati personali degli altri vanno trattati con cura, come richiede la legge.



Tratta con cura i dati personali.

4.3 Se succede

L'ultima lezione è la più concreta: che cosa fare se succede, anche quando le difese non bastano.



Prepararsi aiuta a sapere che cosa fare.

Ecco il percorso completo del corso, in un colpo d'occhio.



Il percorso del corso: da che cosa ci difendiamo, come, e che cosa fare se succede

5. Come seguire il corso

Ogni lezione ha quattro materiali, che dicono le stesse cose in modi diversi: puoi scegliere quello che ti viene meglio.

- **La dispensa** (PDF): da leggere con calma e da conservare;
- **Le slide**: per ripassare o per spiegare agli altri;
- **Il video**: per capire in fretta i punti principali;
- **L'esercitazione**: la parte più importante, da fare con quello che hai già.

Il consiglio è semplice: leggi la dispensa, guarda il video, poi fai l'esercitazione. Una lezione alla volta, senza correre. Se dopo una settimana ti ricordi il metodo ma non i dettagli, va benissimo: i dettagli si ritrovano nella dispensa.



Nove lezioni, una alla volta: leggi, guarda e prova.

Quando senti di aver capito il metodo, scarica la dispensa gratuita su gianlu.it e passa alla lezione successiva.

> **UN RITMO CHE FUNZIONA**
>
> Una lezione per volta, con una pausa fra l'una e l'altra per provare le cose sul tuo computer. Chi mette in pratica la lezione 5 (le password) il giorno stesso se la ricorda per anni.

6. Chi te lo racconta

Sono Gianluca Bonomo, consulente informatico e formatore. Da anni spiego il digitale a chi non è tecnico, con parole semplici ed esempi presi dal lavoro di tutti i giorni. Trovi altri corsi e articoli su www.gianlu.it; per domande o suggerimenti scrivi a info@gianlu.it.

Preparazione

Prima di cominciare, prepara il necessario.

1. Crea sul computer una cartella chiamata «Corso sicurezza» e dentro una cartella per ogni lezione.
2. Apri un file di testo e scrivi una frase: «Voglio proteggere...». Completala con il dato o il servizio che per te conta di più.
3. Controlla di avere Windows 11 aggiornato e un telefono con cui ricevere codici.
4. Scarica la dispensa della lezione 1.

> **ATTENZIONE**
>
> Hai una cartella per ogni lezione?
>
> Sai che cosa vuoi proteggere per primo?

Le domande che arrivano in aula

Devo essere esperto di computer?

No. Il corso parte da zero e spiega ogni termine tecnico la prima volta che compare.

Posso saltare qualche lezione?

Meglio di no: ogni lezione si appoggia sulle precedenti. Se un argomento lo conosci già, leggi la dispensa e passa subito all'esercitazione.

Vale anche per chi usa un Mac o un telefono?

I concetti sì, perché phishing, password e backup sono uguali ovunque. I percorsi dei menu e gli esempi pratici invece sono quelli di Windows 11.

Serve pagare qualcosa o installare programmi?

No: il corso usa quello che hai già, in particolare Sicurezza di Windows. Dove servirebbe altro, te lo dico nella lezione.

Glossario

Termine	Che cosa significa
Backup	Copia di sicurezza dei dati, da usare in caso di perdita o guasto.
Dato personale	Qualunque informazione che riguardi una persona identificata o identificabile.
Malware	Software dannoso creato per danneggiare un computer o rubare dati.
Phishing	Un inganno per convincerti a cliccare un link, aprire un allegato o dare dati riservati.
Verifica in due passaggi	Un secondo controllo, oltre alla password, per entrare in un servizio.

Per approfondire

Gianluca Bonomo, www.gianlu.it - materiali del corso

> **ATTENZIONE**
>
> Esempi, nomi e domini del corso sono di fantasia. Gli esempi pratici fanno riferimento a Windows 11.