



Conclusioni

Che cosa hai imparato e da dove ricominciare domani

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



Indice

Come usare questa dispensa 3

1. Il percorso in breve 3

2. Le conclusioni 5

3. Gli errori più comuni da evitare 7

4. E adesso? 7

4.1 La prima settimana 8

4.2 Il primo mese 8

4.3 Come continuare a imparare 9

Autovalutazione 10

Le domande che arrivano in aula 11

Glossario 11

Per approfondire 12

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**
>
> Ripassare il percorso lezione per lezione, fissare le idee che restano, evitare gli errori più comuni e uscire con un piano d'azione concreto.

Che cosa saprai fare alla fine

- Ricordare l'idea chiave di ogni lezione.
- Riconoscere gli errori più frequenti e come evitarli.
- Valutare la propria situazione con una lista di controllo.
- Pianificare i primi passi: la prima settimana e il primo mese.

1. Il percorso in breve

Sei arrivato fino in fondo. Rimettiamo in fila quello che hai imparato.



Dalle minacce alle difese, fino alla risposta agli incidenti.

Lezione	Idea chiave	Che cosa sai fare ora
1. Che cos'è la sicurezza informatica	Si proteggono riservatezza, integrità e disponibilità; il rischio principale è l'errore umano	Spiegare che cosa devi proteggere e perché
2. Malware e ransomware	Il riscatto non si paga: la difesa è il backup	Riconoscere i tipi di malware e come arrivano
3. Phishing e le sue varianti	Cambia il canale, non l'obiettivo: fermati e controlla	Smascherare e-mail, SMS, telefonate e QR truffa
4. Siti trappola e inganni	L'indirizzo conta più dell'aspetto della pagina	Controllare un dominio e riconoscere l'ingegneria sociale
5. Password e verifica in due passaggi	Frase lunga, una per servizio, secondo controllo	Creare password solide e attivare la verifica
6. Proteggere dispositivi e reti	Aggiornamenti, Sicurezza di Windows, blocco schermo, cifratura	Mettere in sicurezza computer, chiavette e Wi-Fi
7. Il backup e la regola 3-2-1	Tre copie, due supporti, una fuori sede	Organizzare e provare le copie di sicurezza
8. Privacy e protezione dei dati	Solo i dati necessari; violazione da notificare in tempo	Applicare le buone prassi e gestire una violazione
9. Che cosa fare se succede	Isola, avvisa, cambia, segnala	Reagire senza improvvisare

Il percorso, lezione per lezione.

Il filo è uno solo: le minacce (lezioni da 1 a 4) sfruttano quasi sempre una **distrazione**, le difese (da 5 a 8) servono a ridurre il danno quando la distrazione c'è stata, e l'ultima lezione ti dice che cosa fare quando le difese non bastano.



Il percorso fatto: dalle minacce alle difese, fino alla reazione

2. Le conclusioni

Se dovessi ricordare solo quattro cose, sarebbero queste.

1. **L'errore umano è il rischio principale, quindi la formazione è la difesa migliore** (lezione 1). Non serve essere tecnici, serve fermarsi un momento.
2. **Fermati e controlla** (lezioni 3 e 4). Mittente, fretta, link e allegato: quattro domande bastano a fermare la maggior parte delle truffe.
3. **Le difese si sommano** (lezioni 5, 6 e 7). Password lunghe e verifica in due passaggi, aggiornamenti, Sicurezza di Windows, backup con la regola 3-2-1: nessuna è perfetta, insieme funzionano.
4. **I dati sono delle persone** (lezioni 8 e 9). Trattali con cura e, se qualcosa va storto, avvisa subito: il tempo conta.



Formazione, attenzione, difese complementari e cura delle persone.

L'IDEA IN UNA RIGA

La sicurezza non è un prodotto che si compra: è un'abitudine che si costruisce.



Fermati, verifica, proteggi i dati e avvisa presto.

3. Gli errori più comuni da evitare

Sono quelli che ricorrono più spesso nelle domande delle lezioni.

Errore	Che cosa fare invece
Cliccare perché il messaggio mette fretta	Fermarti, controllare il mittente e chiamare l'ente con il numero ufficiale
Usare la stessa password ovunque	Una frase lunga diversa per ogni servizio, in un gestore di password
Rimandare gli aggiornamenti	Lasciarli automatici
Avere un solo backup, sullo stesso computer	Applicare la regola 3-2-1 e provare il ripristino
Pagare il riscatto del ransomware	Ripristinare dalle copie e segnalare
Cercare di «sistemare da solo» un incidente	Isolare il computer e avvisare il responsabile

Gli errori più frequenti.



Riconosci gli errori che possono indebolire le altre difese.

4. E adesso?

Un corso serve se cambia quello che fai domani. Ecco un piano semplice.



Il piano d'azione

4.1 La prima settimana

- attiva la verifica in due passaggi sulla posta e sul cloud;
- cambia le password più importanti con frasi lunghe e diverse;
- controlla che Sicurezza di Windows e gli aggiornamenti automatici siano attivi;
- prendi l'abitudine di premere Windows più L quando ti alzi.

4.2 Il primo mese

- organizza il backup con la regola 3-2-1 e prova a ripristinare un file;
- rivedi chi può vedere quali dati nel tuo lavoro;
- scrivi su un foglio i quattro passi da seguire se succede un incidente e a chi telefonare;
- racconta ai colleghi una cosa che hai imparato.



Questa settimana proteggi gli accessi e aggiorna; questo mese prova backup e piano.

4.3 Come continuare a imparare

Le minacce cambiano, i principi no. Rileggi di tanto in tanto le dispense, guarda i siti ufficiali del Garante per la protezione dei dati personali (www.gpdp.it) e della Polizia Postale e delle Comunicazioni (www.commissariatodips.it), e scrivi a info@gianlu.it se hai dubbi o vuoi un corso su un tema che manca.

Autovalutazione

Una lista di controllo per vedere dove sei. Rispondi sì o no.

1. Ho attivato la verifica in due passaggi sulla posta?
2. Ho una password diversa e lunga per i servizi importanti?
3. Gli aggiornamenti di Windows sono automatici e Sicurezza di Windows mostra le spunte verdi?
4. Ho almeno tre copie dei miei dati, su due supporti, una fuori sede?
5. Ho provato a ripristinare un file dal backup?
6. So che cosa fare e chi avvisare se succede un incidente?

> **ATTENZIONE**
>
> Dove hai risposto no, quella è la tua priorità della prima settimana.

Le domande che arrivano in aula

Da dove comincio se ho poco tempo?

Dalla verifica in due passaggi sulla posta e da una password lunga per il servizio più importante: sono le due mosse che danno più protezione con meno fatica.

Basta aver seguito il corso per essere al sicuro?

No: la sicurezza totale non esiste. Il corso riduce molto il rischio e ti prepara a reagire bene quando succede qualcosa.

Quanto spesso devo ripassare?

Una rilettura delle dispense ogni tanto, e un controllo del backup e degli aggiornamenti ogni mese.

Posso consigliare il corso ai colleghi?

Certo: le dispense sono pensate anche per questo. Una squadra che segue le stesse regole è molto più difficile da ingannare.

Glossario

Termine	Che cosa significa
Backup	Copia di sicurezza dei dati, da usare in caso di perdita o guasto.
Cybersquatting	Registrazione di nomi a dominio simili a marchi altrui per trarne vantaggio.
Firewall	Sistema che filtra il traffico di rete e blocca le connessioni non autorizzate.
GDPR	Regolamento europeo sulla protezione dei dati personali.
Ingegneria sociale	Manipolare le persone, più che le macchine, per ottenere dati o accessi.
Malware	Software dannoso creato per danneggiare un computer o rubare dati.
Phishing	Inganno per carpire dati o far cliccare su link e allegati pericolosi.
Ransomware	Malware che cifra i file e chiede un riscatto.
Regola 3-2-1	Tre copie dei dati, su due supporti diversi, una fuori sede.
Verifica in due passaggi	Un secondo controllo, oltre alla password, per entrare in un servizio.

Per approfondire

Garante per la protezione dei dati personali - www.gpdp.it

Polizia Postale e delle Comunicazioni - www.commissariatodips.it

Sicurezza di Windows - guida integrata nell'app (Start, Sicurezza di Windows)

> **ATTENZIONE**
>
> Questa lezione ricapitola il corso e non introduce argomenti nuovi. Per norme e procedure fai sempre riferimento ai siti ufficiali.