Perchè è finita così?

Perchè è finita così?

- **FIDUCIOSA/INGENUA**

1) PERCHÈ DOVREI ESSERE UN BERSAGLIO?
2) NON PERCEPISCO PERICOLO
3) NON HO TEMPO/BUDGET PER PROTEGGERMI
4) NON SONO “TECNOLOGICO”

Perchè è finita così?

- **FIDUCIOSA/INGENUA**

Perchè è finita così?

- **FIDUCIOSA/INGENUA**
- **NON CONOSCE LE INSIDIE**

1) SEMINO TRACCE / FORNISCO (IN)CONSAPEVOLMENTE DATI AZIENDALI E PERSONALI
2) NON VERIFICO CHI SIA REALMENTE IL MIO INTERLOCUTORE

Perchè è finita così?

- **FIDUCIOSA/INGENUA**
- **NON CONOSCE LE INSIDIE**

1) LE RACCOLGO TUTTE E LE METTO IN RELAZIONE. TI COLPISCO GRAZIE AL TUO AIUTO
2) MI NASCONDO/MIMETIZZO BENE E CONTINUO A MIGLIORARMI

1) SEMINO TRACCE / FORNISCO (IN)CONSAPEVOLMENTE DATI AZIENDALI E PERSONALI
2) NON VERIFICO CHI SIA REALMENTE IL MIO INTERLOCUTORE

Perchè è finita così?

- **FIDUCIOSA/INGENUA**
- **NON CONOSCE LE INSIDIE**
- **NON HA ASCOLTATO I CONSIGLI**

1) LA CYBER SECURITY È UNA BUZZWORD. UN COSTO NON INVESTIMENTO

Perchè è finita così?

- **FIDUCIOSA/INGENUA**
- **NON CONOSCE LE INSIDIE**
- **NON HA ASCOLTATO I CONSIGLI**

1) NON ATTUARLA POTREBBE COSTARTI MOLTO DI PIÙ. CHI NON SI PROTEGGE È UNA FACILE PREDA.

1) LA CYBER SECURITY È UNA BUZZWORD. UN COSTO NON INVESTIMENTO

BUONE PRATICHE – Lato Azienda

CONSAPEVOLEZZA	• **Creare un inventario** di tutti i sistemi, dispositivi e software in uso dall'azienda. **Fare attenzione al lavoro da remoto** • **Individuare i sistemi critici.** COSA È REALMENTE STRATEGICO • **Valutare i costi** (tutti!) in caso di cyber attacco
AZIONE	• **Nominare un referente che sia IN-FORMATO** • **Creare policy aziendale di cyber security (cosa e chi deve fare / provare il piano)** • **Sensibilizzare tutti gli utenti a non usare le risorse informatiche aziendali per scopi personali** • **Formare e mantenere aggiornato il personale** • **Installare antivirus, firewall, aggiornare software** • **Fare il backup** (regola 3,2,1) • **Proteggere il sito web** • **Utilizzare il più possibile l'autenticazione a due fattori**

BUONE PRATICHE – Lato Utente

PASSWORD	• NO password comuni (es. “123456” o “qwerty”); • NO password con dati personali • **Almeno 12 caratteri**, combinare lettere minuscole e maiuscole, numeri e caratteri speciali, in maniera casuale, senza rispettare gli “schemi comuni” e scegliere caratteri speciali di utilizzo meno frequente (es. [,£,]) • La password di accesso/sblocco PC, per comodità, può essere meno “casuale” (es. una breve frase) • **Non usare una sola password per più account**: password sicure e diverse per ogni log-in • Cambiare la password ciclicamente (ogni 90gg) • Tenerle al sicuro: (con Password Manager = gestore di password, o cartacee ma sottochiave) • Non lasciare la postazione di lavoro senza aver messo il PC in lock • Non inviate (a colleghi) le password via mail. Al vostro rientro in ufficio cambiate le password
COMPORTAMENTI	• Se notate che il vostro PC è diventato più lento, o si aprono schermate strane, informate subito il Responsabile • Non inserite mai chiavette USB di dubbia provenienza nel vostro PC

BUONE PRATICHE – Lato Utente

PHISHING	• **Sempre massima attenzione quando aprite una mail** • **Verificate mittente**: i parametri “Reply-to” e “Return-Path” devono portare allo stesso dominio indicato nell’email. • **Non fatevi reindirizzare**: senza cliccare, muovete il mouse sopra i link per vedere dove puntano • **Non aprite allegati** se non siete certi del mittente
NAVIGAZIONE ON LINE	• **Siate consapevoli dei dati sia aziendali che personali che condividete** anche, e in special modo, quelli sui social. • Fornite il minor numero di dati possibili (es. form iscrizione) • Assicuratevi di visitare solo siti protetti (HTTP**S**) differentemente siate accorti a non scaricare file. • Ricordatevi sempre di effettuare il logout (siti per i quali avete un account) • Non utilizzare reti internet di cui non si conosce il livello di sicurezza, soprattutto nel caso in cui si debba accedere a servizi personali, server aziendali o fare acquisti. Disabilitate la funzione di accesso automatico alle reti Wi-Fi disponibili. • Non usate reti WI FI free per operazioni strategiche (home banking, fascicoli sanitari, firme digitali, ecc..)