CHECK LIST
Sicurezza informatica.

HORTISECUR

Come proteggersi dai criminali informatici!

1. Dispositivi e software

- ☐ Aggiornare regolarmente PC, laptop e tablet
- ☐ Mantenere aggiornati sistemi operativi, software di controllo e app
- ☐ Installare un programma antivirus su tutti i dispositivi
- ☐ Proteggere Wi-Fi e router con una password sicura (non usare password predefinite)

2. E-mail e comunicazione

- ☐ Aprire allegati e link nelle e-mail solo se il mittente è conosciuto e attendibile
- ☐ Eliminare immediatamente le e-mail sospette – non cliccare mai sui link!
- ☐ Informare i collaboratori sui pericoli informatici (formazione e opuscolo informativo)
- ☐ Controlli regolari: ci sono e-mail che sembrano strane o false?

3. Dati di accesso

- ☐ Assegnare una password complessa e unica per ogni sistema (e-mail, contabilità, negozio online, ecc.)
- ☐ Non annotare le password sullo schermo o sotto la tastiera
- ☐ Autenticazione a due fattori (2FA) attivata, ove possibile (ad es. per l'online banking)

4. Backup dei dati

- ☐ Backup regolare di tutti i dati importanti (ad es. elenco clienti, documenti, sistemi di controllo)
- ☐ Backup su supporto esterno (non sempre connesso a Internet)
- ☐ Il ripristino del backup è già stato testato?

5. Organizzazione e preparazione

- ☐ Designare un referente per le questioni IT in azienda
- ☐ Sviluppare un piano di emergenza: cosa fare in caso di attacco da virus o e-mail sospette?
- ☐ Tutti i collaboratori sono stati informati: in caso di dubbio, meglio chiedere piuttosto che cliccare

6. Dispositivi connessi a Internet in azienda (IoT)

- ☐ Garantire la sicurezza di dispositivi come sensori, sistemi di climatizzazione o impianti di riscalda-mento
- ☐ Modificare password predefinite
- ☐ Utilizzo esclusivo di produttori affidabili
- ☐ Attivare l'accesso da remoto solo con password + controllo di sicurezza

Suggerimento

Una volta al trimestre, rivedere brevemente tutti i punti: piccoli passi aiutano a prevenire danni ingenti.

www.hortisecur.it