Lamberti

Le Buone Pratiche Digitali

La nostra sicurezza dipende da te

luglio 2021

Per essere sicuri, nella vita di tutti i giorni prendiamo delle precauzioni.

Usciamo prima di casa se c’è traffico, prendiamo l’ombrello se sono previsti temporali, usiamo le presine per scolare la pasta. Non diamo le nostre chiavi di casa ad uno sconosciuto che ci ferma per strada e quando notiamo un comportamento strano ci allarmiamo. La sicurezza è una priorità nella vita privata come in quella lavorativa: usiamo l’elmetto, passeggiamo sui camminamenti, non scendiamo le scale guardando il nostro telefonino.

Nella vita di tutti i giorni, ciascuno di noi è attento alla propria **“sicurezza”** e a quella dei propri cari. Dobbiamo esserlo anche durante la nostra **presenza in Rete, a casa come in azienda**, consapevoli dei rischi e dei pericoli. Seguire poche chiare regole ci aiuta a proteggerci e insieme a proteggere il nostro Gruppo. **Perché il rischio cyber cresce e dobbiamo essere tutti più attenti.**

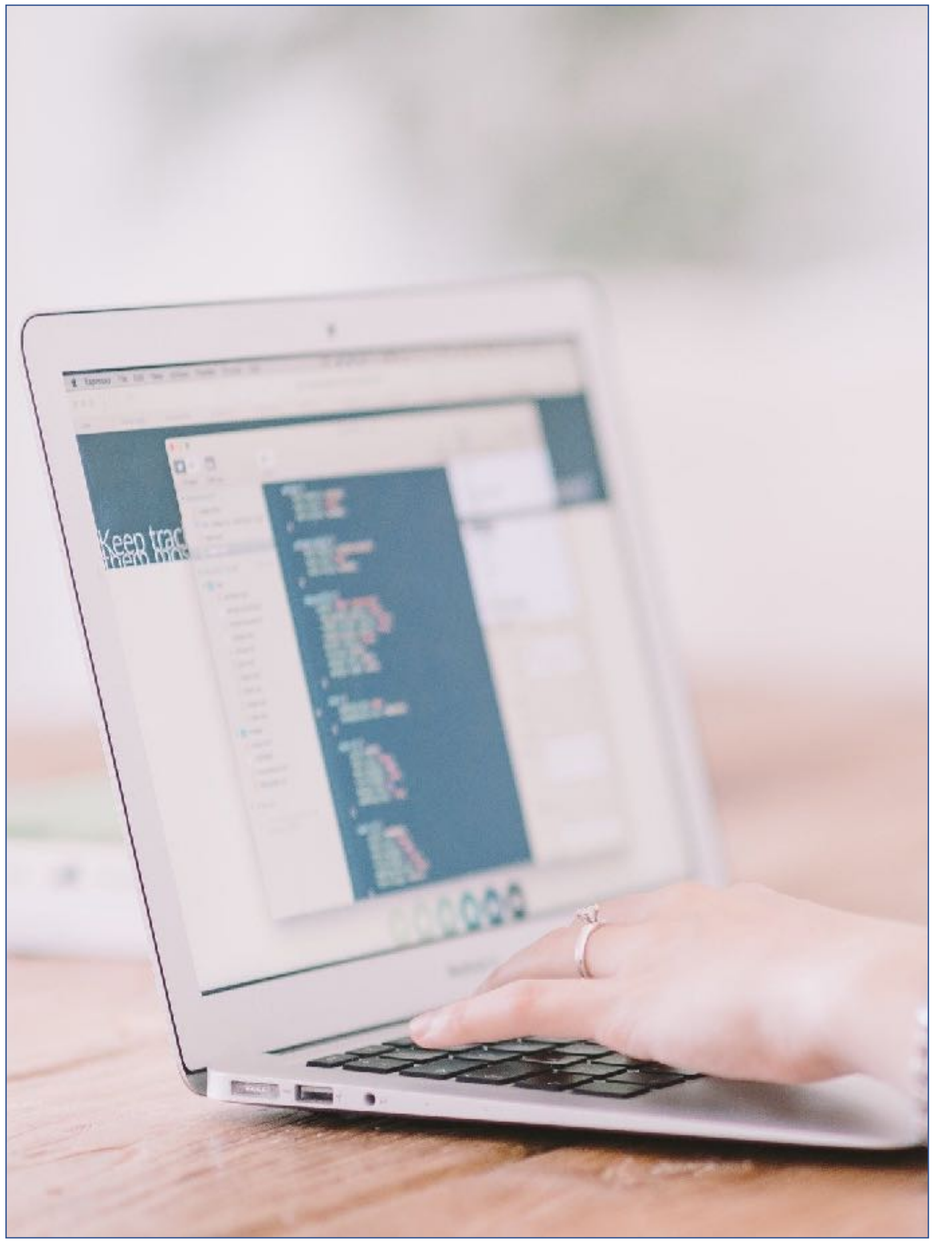
Occhio alle tue Password!

La password che usi sul lavoro deve essere univoca e non deve assomigliare a quelle che usi nella vita privata.

Se sei in dubbio utilizza una frase per te importante o facile da ricordare come ad esempio “miamammahaicapellirossi”. Cambia la tua password frequentemente e in maniera completa (non aggiungere numeri a quella esistente ma usane una diversa).

Utilizza password diverse per accedere alla rete aziendale, SAP, Zucchetti ecc. Così se una password viene compromessa le altre restano al sicuro. Non dare ad altri le tue password.

La posta elettronica...



... non è un mezzo così sicuro come pensiamo. Non utilizzarla per inviare informazioni sensibili quali password, IBAN, dati di carta di credito, richieste personali, ecc.

Usa la mail aziendale solo per le comunicazioni di lavoro. Se devi inviare dei file che contengono informazioni riservate, proteggili sempre con una password e comunicala al destinatario con uno strumento differente dalla mail (es. via SMS o WhatsApp). Non dare seguito ad alcun messaggio che richieda di accedere a pagine web esterne e all'inserimento delle tue credenziali. Non rispondere ad alcun messaggio che ti sembra sospetto o fraudolento e segnalalo subito ai nostri servizi informatici **ictsecurity@lamberti.com**. Non rispondere a messaggi provenienti da indirizzi generici come ad esempio info@ or ufficio.commerciale@

Chi mi scrive?

Non fermarti al nome del mittente che visualizzi sul messaggio di posta elettronica.

Controllalo cliccandoci sopra per verificare l’indirizzo per esteso. Cancella tutte le mail di cui non riconosci il dominio. Fai attenzione, può succedere che qualcuno si inserisca anche in scambi autentici.

Leggi bene il testo

Nel testo della mail o di un sms ci sono errori di grammatica? Frasi strane? Sintassi anomala?

Potrebbero essere indizi utili per identificare una mail fraudolenta.

Non agire e contatta i nostri servizi informatici
ictsecurity@lamberti.com

Nuove istruzioni? Fermati!

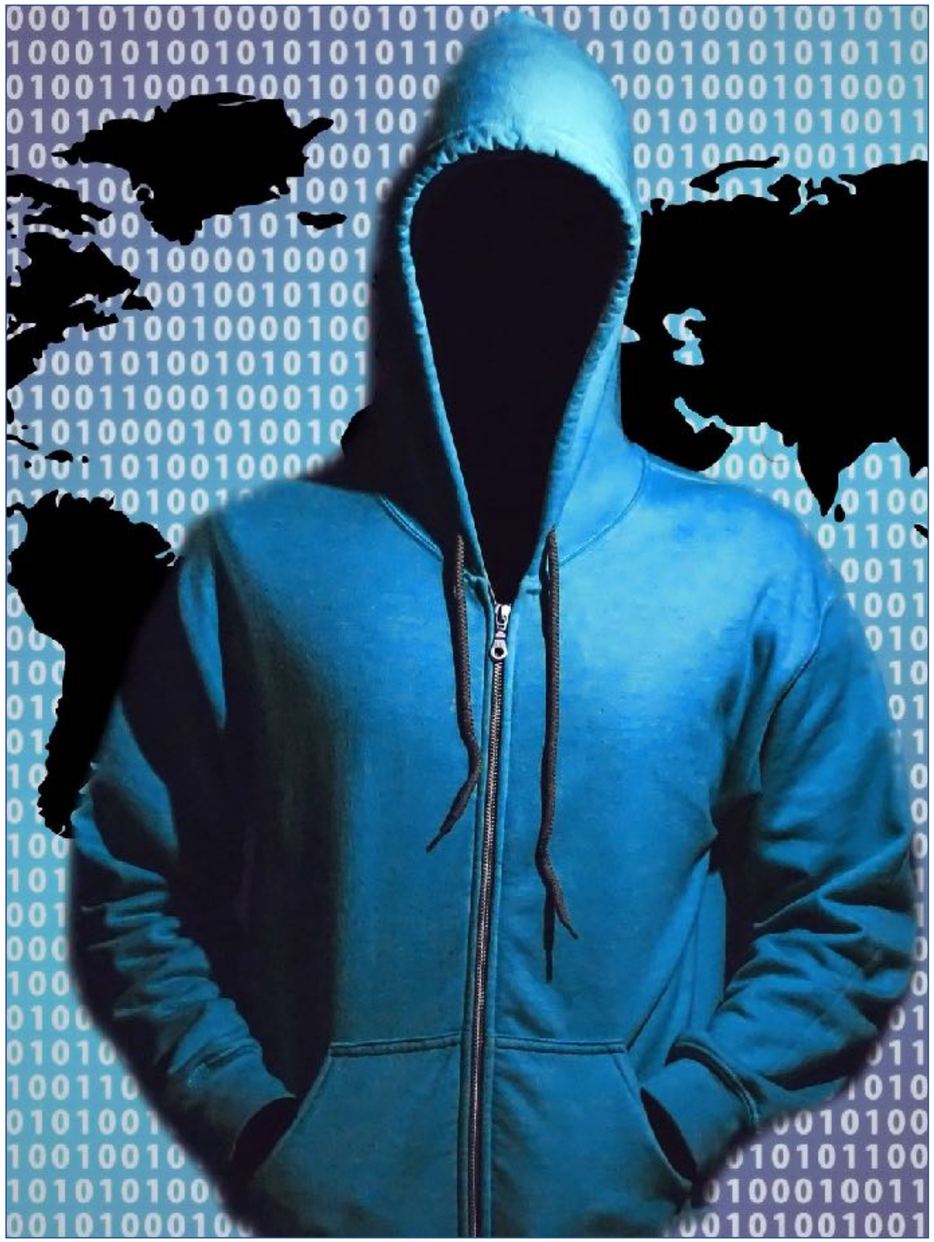
Hai ricevuto una mail da un cliente, da un contatto in azienda anche se apicale, da un fornitore con nuove istruzioni IBAN, richiesta di modifiche dei dati bancari, richiesta di trasferimenti fondi urgenti, modifiche alle usuali modalità di acquisto e vendita del Gruppo Lamberti?

Non dare mai seguito alle richieste prima di aver contattato telefonicamente il nostro Ufficio Amministrazione che provvederà a verificare l'autenticità della comunicazione.

Non cliccare sui link

Hai ricevuto una mail, un messaggio WhatsApp o SMS che ti chiede di donare fondi? Una catena di Sant'Antonio? La notifica di un premio vinto? L'invito a partecipare ad un concorso? Non cliccare sui link e non inoltrare la mail ad amici o colleghi.

Dietro ai link si celano truffe, trappole e hacker informatici. Informa subito i nostri servizi informatici **ictsecurity@lamberti.com** anche se ti sei distratto e hai cliccato per errore. Se lo fai tempestivamente puoi prevenire un attacco informatico.



Chiavette USB? No Grazie :-)

Da dove viene la chiavetta? Chi l'ha usata per ultimo? Ti è stata regalata? L'hai trovata?

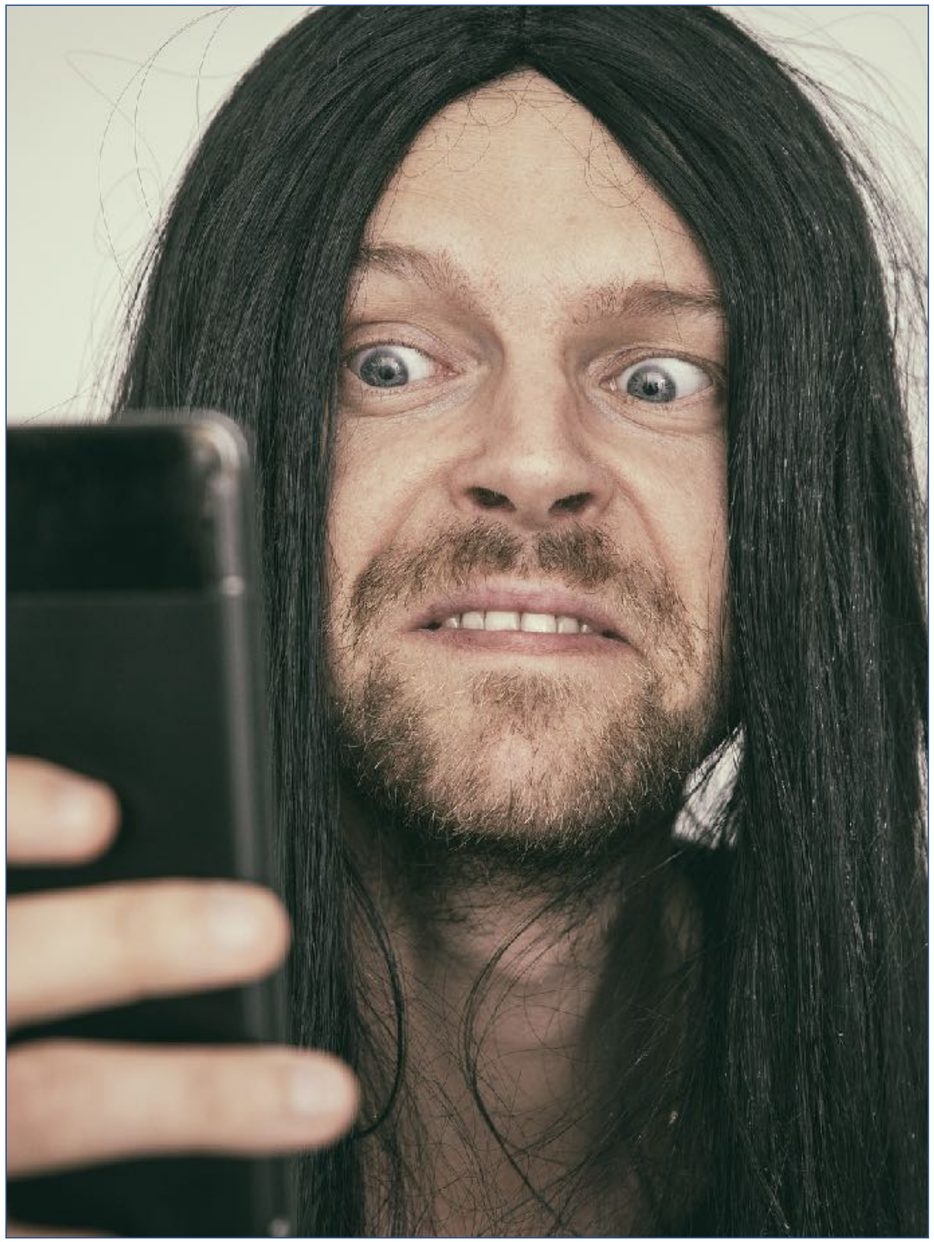
Le chiavette possono diffondere "malware", piccoli programmi software che si diffondono rapidamente e che possono mettere in pericolo la rete aziendale. Non utilizzarle nei pc aziendali.

Truffe telefoniche e via SMS/WhatsApp

I criminali informatici sono molto sofisticati. Fai attenzione agli sms, messaggi WhatsApp che ricevi con link e alle telefonate con richieste di informazioni.

Non divulgare password o informazioni non pubbliche senza aver verificato l'identità dell'interlocutore anche quando sembra un collega o un fornitore di servizi (fornitore energia elettrica, gas, telefonia, banca, assicurazione...).

Se ricevi un sms da un numero che non conosci digitalo in rete e verifica se ci sono commenti da parte di altri utenti.

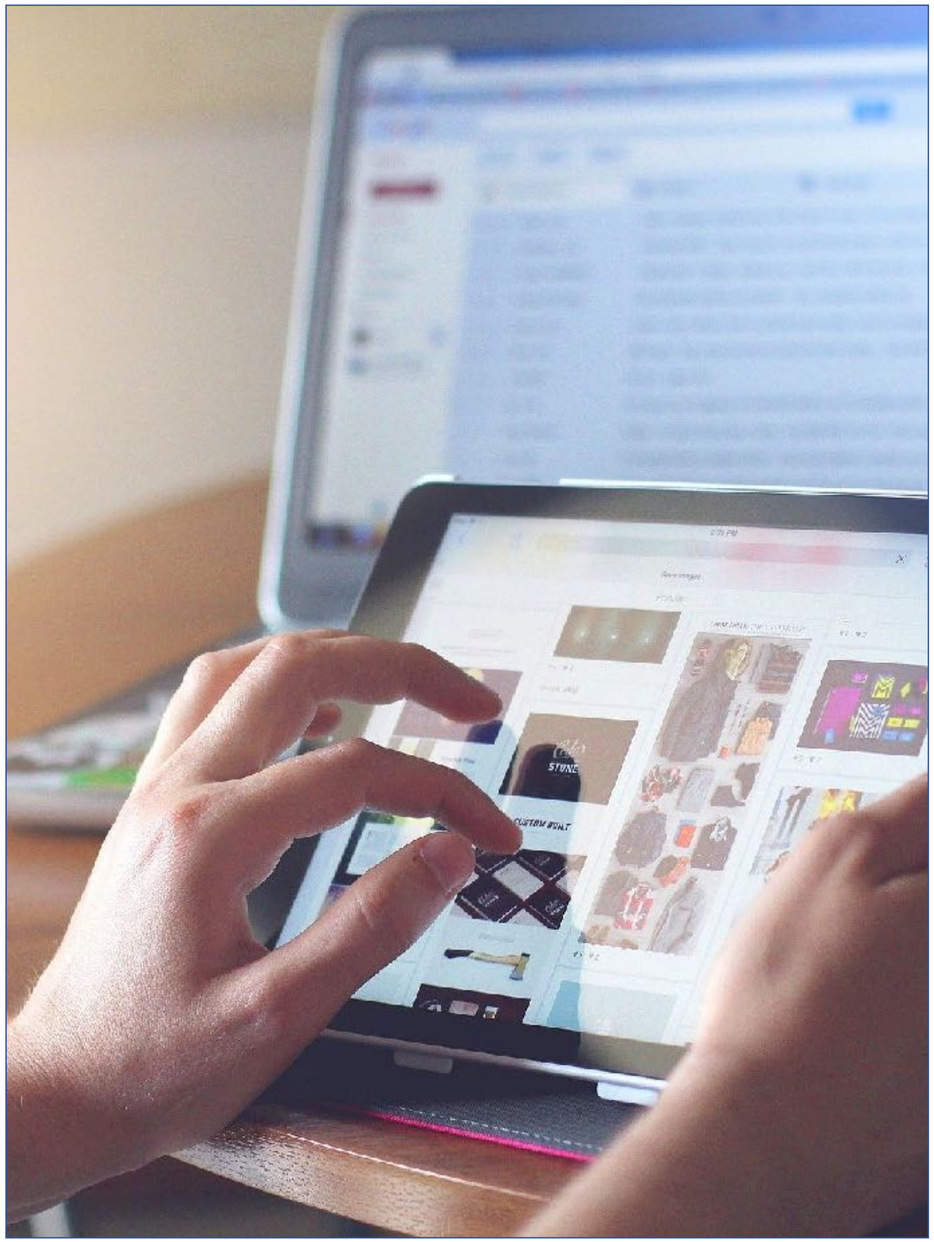


Vigile quando navighi in rete

Non fermati al lucchetto di fianco all'indirizzo, cliccaci sopra e assicurati che il nome coincida con l'indirizzo; possibilmente riscrivi l'indirizzo evitando i link che non mostrano dove ti portano.

Fai attenzione ai siti e alla navigazione in generale, basta una disattenzione, un clic sbagliato, una pagina rimasta aperta. Verifica sempre l'indirizzo, non farti prendere dalla fretta o dalla curiosità.

Se qualcosa sembra non funzionare a dovere, segnalalo **ictsecurity@lamberti.com**, potrebbe essere un indizio di un tentativo di intrusione.



Sito autentico o truffa?

Esistono siti cloni o truffa che sembrano autentici.

Ecco alcuni elementi che ti aiutano ad identificare un possibile sito clone/truffa: **mancanza di indicazione dei dati del venditore** (sede, telefono, partita IVA, iscrizione al registro delle imprese, etc.), **errori grammaticali o di ortografia nei testi del sito, mancanza di informativa privacy o di condizioni generali di vendita, modalità di pagamento insolite** (ad es. accettazione del solo bonifico bancario), **utilizzo di un nome per il sito non attinente all'attività svolta** (ad es. un nome legato al cibo per un sito che vende scarpe), **vendita di prodotti di marca** (specie nel settore abbigliamento) **a prezzi estremamente vantaggiosi/ fuori mercato**. Si tratta di semplici indizi, che devono però metterti in allerta.

La tua privacy è un bene prezioso!

Controlla sempre le tue impostazioni per sapere quali dati stai rendendo pubblici.

Ad esempio sullo smartphone assicurati che i dati di geolocalizzazione siano attivi solo quando utilizzi determinate applicazioni. Sui social network non geolocalizzare le tue foto, non rendere pubblici i tuoi periodi di viaggio o di vacanza, non concedere amicizia o dare confidenza a chi non conosci, non fornire informazioni personali, non indicare dove abiti o dove lavori.

Fai attenzione alle immagini che posti online.

Lamberti

I comportamenti digitali virtuosi proteggono noi e la nostra azienda.


Lamberti