DigitaleFacile

La tua guida al digitale

2. Vita Digitale

2.9

Proteggere i dispositivi

Finanziato dall'Unione europea NextGenerationEU
REPUBBLICA DIGITALE
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
Regione Lombardia
PUNTO DIGITALE FACILE

Proteggere i dispositivi

Perché proteggere i dispositivi elettronici?

I dispositivi elettronici usati per connettersi a *Internet* (per esempio *computer, tablet* e *smartphone*) possono essere veicolo di trasmissione di *virus informatici* ed essere attaccati da *hacker* allo scopo di carpire dati personali e *credenziali di autenticazione* ai profili bancari. Per questo, è fondamentale utilizzare adeguati sistemi di protezione e precauzioni d'uso.

Poiché si tratta di apparecchi tecnologici molto sofisticati, è anche importantissimo prendersene cura: non esporli a fonti di calore, freddo intenso o umidità che possono compromettere le batterie e le componenti, evitare cadute o urti.

Per proteggere i dispositivi...

...usare password sicure

Assicurarsi sempre che tutti i dispositivi elettronici siano protetti con una *password* sicura (almeno 8 caratteri alfanumerici, maiuscole e minuscole, simboli), che non contenga date o nomi riconducibili all'utente o a membri della sua famiglia e che sia custodita in luogo sicuro e non accessibile ad altri.

Si raccomanda di cambiare la password periodicamente, almeno una volta ogni 6 mesi.

...utilizzare sempre un *lockscreen*

Tutti i dispositivi permettono di impostare una password o un *PIN* per l'accesso ai dati contenuti.

Il blocco dello schermo è importante per tutelare la riservatezza delle informazioni soprattutto in caso di smarrimento o furto del *device*.

...installare software antivirus e antiphishing

L'*antivirus* è un programma informatico in grado di individuare e rimuovere i *malware* che, tramite la rete, possono contagiare il dispositivo elettronico, mentre l'*antiphishing* è un software specifico per identificare le *e-mail* truffa.

A questo proposito è bene ricordare di non aprire mai messaggi di posta elettronica provenienti da mittenti sconosciuti, che presentano errori di ortografia e chiedono l'immissione di dati e informazioni da parte dell'utente. Non aprire nemmeno gli allegati a questi messaggi che possono contenere virus.

...effettuare il *backup* dei dati

È importante effettuare periodicamente una copia di sicurezza dei dati informatici in modo da poterli recuperare in caso di perdita accidentale. Il backup può essere effettuato sia attraverso il *cloud* che su un dispositivo di memoria esterno (a esempio, una *chiavetta USB*). Il backup può interessare documenti, contatti, immagini e *messaggi istantanei*.

...adottare un *firewall*

Il *firewall* è un software che funge da barriera per i virus. A differenza dell'antivirus, che interviene a "curare" il dispositivo contagiato, questo è un sistema di sicurezza di rete che autorizza o blocca a monte la trasmissione di dati se considerati pericolosi per il dispositivo.

Proteggere i dispositivi

Si tratta di una precauzione importantissima soprattutto se il device è collegato in rete con altri dispositivi.

...navigare in sicurezza

In Internet si trova davvero di tutto. Per questo è essenziale fare attenzione ai siti che si visitano e ai programmi che si scaricano dalla rete. Verificare che l'indirizzo del sito inizi con "https" (significa che il sito è protetto e certificato come lo sono, a esempio, i siti delle banche) e che presenti l'immagine di un lucchetto. Cliccando sul lucchetto è anche possibile ottenere informazioni sul tipo di codifica utilizzata a protezione del sito.

...tutelare i propri dati personali

Sembra scontato, ma spesso si condividono dati e informazioni in rete. Un esempio? I *social network*, ma anche siti di *e-commerce*, prodotti e servizi che chiedono la registrazione e una serie di informazioni personali per profilare l'utente. Fare quindi sempre attenzione a non condividere informazioni se non si è certi della sicurezza del sito.

Da sapere...

Nel caso in cui si sospetti o si abbia la certezza che i propri dati siano stati violati, è possibile rivolgersi al *Garante per la protezione dei dati personali* o, nei casi più gravi, alla *Polizia Postale*.

GLOSSARIO

ANTIPHISHING – Soluzioni che proteggono gli utenti dal tentativo di ottenere informazioni sensibili attraverso tecniche ingannevoli (es. e-mail o siti web falsi).

ANTIVIRUS – Programma informatico che, in base a diversi livelli di protezione, rileva, blocca e rimuove virus da strumenti elettronici collegati alla rete internet.

BACKUP – Procedimento tramite il quale si effettua una copia di sicurezza di tutti i dati presenti in un computer.

CLOUD – Servizio che consente agli utenti di poter disporre di uno spazio di archiviazione per documenti informatici accessibile in ogni luogo.

COMPUTER – Dispositivo elettronico in grado di elaborare informazioni.

CREDENZIALI DI AUTENTICAZIONE (O ACCESSO) – Generalmente costituite dal nome utente e dalla password. Consentono l'ingresso a siti/servizi.

DEVICE – Dispositivo elettronico. Nel gergo comune, computer, stampante, smartphone, tablet, ecc.

DISCO FISSO – Rappresenta il sistema principale di memoria di un computer. Ogni dispositivo ne ha uno interno, ma esistono anche dischi esterni che possono essere collegati all'apparecchio per aumentare lo spazio di archiviazione.

E-COMMERCE (Electronic Commerce) – Attività di compra-vendita effettuata attraverso siti internet.

E-MAIL – In italiano posta elettronica, è un mezzo di comunicazione che permette di recapitare messaggi, anche con allegati, tramite internet.

FIREWALL – Sistema di protezione e filtro delle informazioni da e per Internet. La sua attivazione blocca l'accesso a contenuti potenzialmente pericolosi.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI – Autorità di controllo che vigila sul rispetto della normativa europea e nazionale in tema di trattamento dei dati.

HACKER – Esperto di programmazione informatica che viola le reti di computer per compiere atti illeciti, come ad esempio carpire informazioni personali e credenziali di accesso per entrare nei siti protetti (es. banca).

INTERNET – Rete di dispositivi che consente lo scambio di informazioni a livello mondiale.

LOCKSCREEN – Schermata di blocco di un dispositivo. Senza una password o un PIN il dispositivo non è accessibile.

MALWARE – Termine che indica virus informatici dannosi per i dispositivi elettronici.

Proteggere i dispositivi

MESSAGGI ISTANTANEI – Brevi testi scambiati in tempo reale fra due o più soggetti che utilizzano dispositivi elettronici connessi alla rete (computer, tablet, smartphone).

PASSWORD – Parola d'ordine composta da caratteri alfabetici, numerici e simboli, creata per proteggere l'accesso a computer e servizi digitali.

PIN (Personal Identification Number) – Codice di 4 cifre associato a una SIM Card che consente lo sblocco dello smartphone.

POLIZIA POSTALE – Area specializzata della Polizia che si occupa dei crimini informatici e dei reati che avvengono per mezzo della rete.

SMARTPHONE – Significa "telefono intelligente". Grazie al sistema operativo unisce le caratteristiche di un telefono con quelle di un computer.

SOCIAL NETWORK (Facebook, Instagram, X, Linkedin, Tik Tok, ecc.) – Comunità di soggetti che condividono messaggi, foto, ecc. a quanti fanno parte della stessa rete. Per accedervi è necessaria una registrazione. La condivisione dei contenuti è possibile fra soggetti collegati fra loro.

TABLET – Apparecchio elettronico connesso ad internet le cui dimensioni dello schermo sono maggiori a quelle di uno smartphone ma inferiori a quelle di un computer (ad es. IPad, Galaxy Tab, MatePad, ecc.).

USB – In questo contesto, apparecchio mobile che consente l'archiviazione di documenti e dati da un computer.

VIRUS INFORMATICI – Programma che si installa in modo involontario sugli strumenti elettronici causando perdita di dati e danneggiamento dei sistemi.

Per maggiori informazioni

Per maggiori informazioni sulle modalità di protezione dei dispositivi informatici, rivolgersi ai facilitatori digitali.

www.regione.lombardia.it

Finanziato dall'Unione europea NextGenerationEU
REPUBBLICA DIGITALE
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
Regione Lombardia
PUNTO DIGITALE FACILE