CYBER SECURITY

Come proteggere il tuo mondo digitale

Provincia di Biella
Materiale realizzato dalla volontaria del Servizio Civile Digitale

Provincia di Biella
Servizio Transizione Digitale

Che cos'è la Cybersecurity?

Per cybersecurity s'intende quel ramo della sicurezza informatica che comprende gli strumenti e le tecnologie usati per proteggere i sistemi digitali (inclusi software, hardware e dati) dalle minacce esterne.

Provincia di Biella

Servizio Transizione

Perchè la Cybersicurezza è Importante?

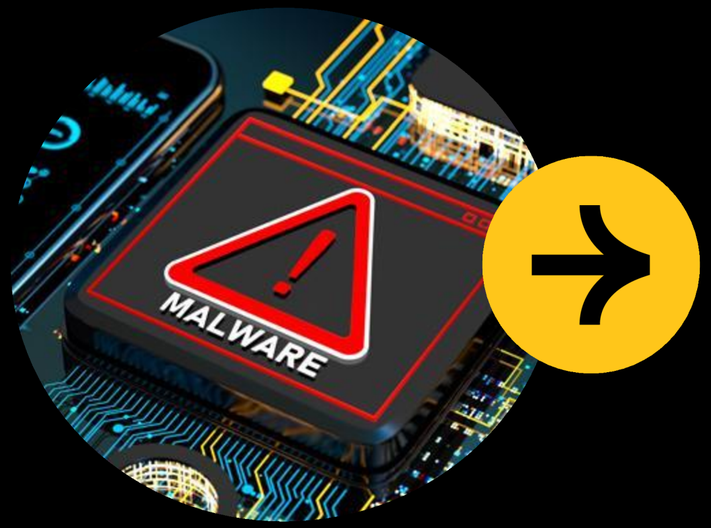
- Protegge i dati personali
- Previene il furto di identità
- Mantiene l'integrità del sistema e dei dati.
- Evita danni finanziari e reputazionali (in ambito aziendale, lavorativo e privato)

Provincia di Biella
Servizio Transizione Digitale

Minacce informatiche più diffuse

- Malware (Virus, Ransomware, Trojans)
- Phishing
- Spamming

Provincia di Biella
Servizio Transizione Digitale



Cos'è un Malware ?

Il termine "malware" viene utilizzato per indicare qualsiasi programma o codice dannoso per i sistemi informatici. Questo tipo di software cerca di infiltrarsi, danneggiare o disattivare computer, sistemi informatici, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni di un dispositivo. Le motivazioni dietro il malware possono variare: può essere finalizzato al profitto, sabotare il normale funzionamento, esprimere un'opinione politica o semplicemente vantarsi. Anche se il malware non può danneggiare l'hardware fisico dei sistemi o delle reti, può rubare, crittografare o cancellare dati, alterare o dirottare le funzioni principali di un computer e monitorare le attività informatiche senza autorizzazione.

Provincia di Biella
Servizio Transizione Digitale

Alcuni tipi di malware

VIRUS INFORMATICO - è un tipo di malware che si attacca ad altri programmi, si replica e infetta altri file con il proprio codice dannoso.

TROJAN - è uno dei tipi di malware più pericolosi. Si presenta come qualcosa di utile per ingannare l'utente. Una volta che si trova sul sistema, gli aggressori ottengono l'accesso non autorizzato al computer interessato. I Trojan possono essere utilizzati per rubare informazioni finanziarie o installare altre forme di malware (es. ransomware).

RANSOMWARE - è un tipo di malware che blocca l'accesso ai dispositivi e/o cripta i file, richiedendo un riscatto in criptovalute. È un attacco difficile da difendere e può essere inflitto facilmente online. Gli attacchi ai singoli consumatori sono attualmente in calo mentre quelli alle aziende sono in aumento

Provincia di Biella

Servizio Transizione Digitale

Come rimuovere il malware

1. Assicurarsi di installare un efficace programma di sicurezza informatica.
2. Effettuare una scansione con un antivirus. Anche le versioni gratuite sono valide per eliminare il malware, ma non offrono una protezione proattiva.
3. Modificare tutte le password, non solo per il PC o il dispositivo mobile, ma anche per l'email, i social media, i servizi bancari e di fatturazione online.

Con spyware, trojan bancari e altre minacce, non è possibile sapere con certezza quali dati siano stati compromessi prima di rimuovere l'infezione. L'uso di un'autenticazione a più fattori (almeno a due fattori) e di un gestore di password è consigliato per la sicurezza.

Nel caso di infezioni da malware su iPhone o iPad, la situazione è più delicata. Apple non permette la scansione del sistema o dei file del dispositivo. L'unica soluzione è ripristinare il telefono con le impostazioni di fabbrica e recuperare i dati da un backup su iCloud o iTunes. Senza un backup, sarà necessario ricominciare da zero.

Come proteggersi dal malware

Alcuni consigli per difendersi dalle minacce informatiche:

- Prestare attenzione al dominio del sito web.
- Utilizzare password robuste con autenticazione a più fattori. In questo caso può essere utile un gestore per le password.
- Evitare clic su annunci pop-up.
- Non aprire allegati da mittenti sconosciuti.
- Non cliccare su link non verificati su email,sms e anche i su social media.
- Evitare di scaricare da siti non affidabili.
- Scaricare app solo dai negozi ufficiali (come Google Play e AppStore).
- Mantenere software sempre aggiornato.
- Disinstallare programmi non utilizzati.
- Eseguire regolarmente il backup dei dati.
- Utilizzare un programma antivirus.

Provincia di Biella
Servizio Transizione Digitale

Gli attacchi phishing

01 Che cos’è il phishing?

02 Alcune misure di sicurezza

03 Cosa fare dopo un attacco?

Provincia di Biella
Servizio Transizione Digitale

Cos’è il phishing ?

Il phishing è un tipo di truffa effettuata su internet dove un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

La più comune forma di phishing viene fatta attraverso l’invio di un’e-mail o altra comunicazione fraudolenta. Il messaggio è strutturato in modo da ingannare l’utente circa l’affidabilità del mittente. Spesso l’e-mail, che presenta un logo contraffatto di un istituto di credito, invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di sicurezza o di ordine tecnico (soprattutto per i servizi bancari).

Provincia di Biella

Servizio Transizione Digitale

È una delle truffe più diffuse online e si esplica in:

- Nelle e-mail (Phishing)
- Negli sms (Smishing)
- Nelle chiamate (Vishing)
- Nei Wi-Fi (Wiphishing)

Possono essere anche combinate tra di loro!

Provincia di Biella
Servizio Transizione Digitale

Cosa fare per proteggersi

Controllare sempre il link e il mittente ed evita di cliccarci sopra.

Controllare sempre l’ortografia. Presta attenzione alla struttura e al contenuto del messaggio.

Non condividere mai i propri dati sensibili con una terza parte.

Usa solo connessioni sicure. Controlla che la connessione sia HTTPS e verifica il nome del dominio all’apertura di una pagina.

Provincia di Biella

Servizio Transizione Digitale

Cosa fare dopo un attacco?

01

Denunciare l’accaduto alla Polizia Postale

C’è l’opportunità di fare tutto comodamente a casa tramite il loro sito (https://www.commissariatodips.it/)

02

Contattare l’amministratore del portale originale per avvertirlo di quanto accaduto.

03

Cambiare le password e monitorare l’attività dell’account.

Provincia di Biella

Servizio Transizione Digitale

Cos'è lo spamming ?

Lo spamming è l'invio indiscriminato, senza il consenso del destinatario, di messaggi di posta elettronica e/o newsletter. In concreto la casella di posta elettronica viene inondata da decine di e-mail pubblicitarie capaci di porre a rischio il funzionamento del servizio di posta elettronica della vittima.

Provincia di Biella
Servizio Transizione Digitale

Alcuni consigli per evitare lo spam

01 Evitare di fornire l’indirizzo e-mail, tranne per servizi indispensabili

02 Non rispondere a e-mail di spam per evitare di confermare l’attività dell’indirizzo

03 Creare un indirizzo e-mail dedicato per newsgroup e siti web, abbandonabile in caso di spam massiccio.

04 Leggere attentamente le autorizzazioni sui moduli per capire chi può accedere ai dati e per quali fini.

Provincia di Biella

Servizio Transizione Digitale

Conclusioni

La sicurezza informatica, in un mondo digitale sempre più connesso, è fondamentale per proteggere l'integrità personale, finanziaria e di sistema. Minacce come malware, phishing e ransomware possono causare danni significativi se non affrontate correttamente.

Provincia di Biella
Servizio Transizione Digitale

Bibliografia e sitografia

CYBERSECURITY: cosa è e perché è importante. https://www.geeksacademy.it/articolo-15/cyber-security-cosa-e-e-perche-e-importante/

Giovani e cybersecurity. https://www.cybersecurity360.it/cultura-cyber/giovani-e-cyber-security-come-educare-le-nuove-generazioni-alla-sicurezza-informatica/

GDPR Scuola. Parliamo di cybersecurity! Ecco come educare alla sicurezza informatica. https://magazine.gdprscuola.it/articoli/parliamo-di-cybersecurity-ecco-come-educare-alla-sicurezza-informatica/

Malwarebytes. Cos'è il malware? https://www.malwarebytes.com/it/malware

Polizia Postale. Che cos'è il phishing? https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html

Polizia postale. Che cos'è lo spamming? https://www.commissariatodips.it/approfondimenti/spamming/spamming-che-cose/index.html

Provincia di Biella

Servizio Transizione Digitale

GRAZIE PER L'ATTENZIONE!

Provincia di Biella

Servizio Transizione Digitale