Ti prendi cura della tua cyber-igiene?

27 Gennaio 2025

I consigli del Centro Cybersecurity in occasione del Data Protection Day

Il 28 gennaio 2025 si celebra la **Giornata Europea della Protezione dei Dati**, un'importante occasione per riflettere sulla sicurezza delle informazioni personali online e sull'importanza di adottare comportamenti adeguati per la protezione digitale. Ma cosa significa prendersi cura della propria cyber-igiene?

La **cyber-igiene** si riferisce all'insieme di pratiche e comportamenti che ogni utente dovrebbe adottare per proteggere le proprie informazioni digitali e la propria identità online. Così come ci prendiamo cura della nostra salute fisica con una corretta igiene personale, dovremmo fare lo stesso nel mondo digitale per prevenire attacchi informatici, furti di dati e altre minacce alla nostra privacy.

In occasione del Data Protection Day, **Giada Sciarretta** e **Matteo Rizzi** dell'unità "Security & Trust" e Science Ambassador di FBK propongono alcuni **consigli pratici e raccomandazioni per migliorare la propria cyber-igiene**. Giada Sciarretta è esperta in progettazione e analisi di sicurezza di soluzioni di identità digitale, Matteo Rizzi è Security Administrator di FBK con esperienza nella gestione dell'identità e nell'analisi di protocolli di sicurezza.

I consigli pratici per la cyber-igiene

Hai mai usato una delle **password** più comuni del 2024? Secondo NordPass, tra le password più utilizzate in Italia troviamo combinazioni di numeri come 123456 o 12345678, oppure parole come "password", "cambiami" e "juventus". Se ne hai riconosciuta una tra le tue credenziali, è il momento di rivedere le tue abitudini di sicurezza online: è infatti fondamentale utilizzare password robuste e diverse per ogni servizio.

"*Le password sono la prima linea di difesa contro gli attacchi informatici; è quindi importante evitare combinazioni prevedibili come "123456" o "password", preferendo soluzioni più complesse e sicure. Una buona pratica è adottare una passphrase lunga almeno 16 caratteri, contenente lettere maiuscole, minuscole, numeri e simboli speciali. Inoltre, è essenziale non riutilizzare la stessa password per più account*" spiega

Giada Sciarretta.

Un'altra misura essenziale è l'**autenticazione multifattoriale (MFA)**, che aggiunge un ulteriore livello di sicurezza richiedendo un secondo fattore oltre alla password, come un codice generato da un'app di autenticazione o un'impronta digitale. Questo riduce notevolmente il rischio di accessi non autorizzati e garantisce una maggiore protezione anche in caso di furto delle credenziali di accesso. Configurare l'MFA per tutti gli account che lo supportano è una delle migliori strategie per proteggere i dati personali.

Un altro consiglio è l'utilizzo di **alias email**, come quelli offerti da servizi come SimpleLogin, che permette di creare alias temporanei per evitare di esporre il proprio indirizzo principale e proteggere la propria identità digitale. Questi alias possono essere utili per iscriversi a servizi online senza compromettere l'account principale, riducendo la possibilità di ricevere spam o di essere vittime di phishing. Sono una buona forma di protezione anche in caso di eventuali "**data breach** ", che si verifica quando dati personali vengono esposti o rubati a causa di una violazione di sicurezza. Le cause principali di un data breach includono attacchi hacker, configurazioni errate dei sistemi, vulnerabilità software e negligenza umana. Le conseguenze possono essere gravi, con impatti finanziari e reputazionali significativi per individui e aziende. Per proteggersi, è possibile controllare regolarmente se il proprio indirizzo email è stato compromesso su siti come Have I Been Pwned, cambiare subito le password in caso di compromissione e abilitare sempre l'autenticazione multifattoriale per limitare i danni.

"*L'utilizzo di alias email si rivela particolarmente efficace anche per proteggersi da eventuali data breach: infatti se un alias viene compromesso, l'utente può facilmente disattivarlo senza influenzare gli altri account, garantendo così un ulteriore livello di protezione. Inoltre, la separazione tra i vari alias impedisce agli attaccanti di correlare diverse identità digitali, limitando la possibilità di attacchi mirati su larga scala. È infine buona pratica monitorare frequentemente i propri account e attivare notifiche di accesso per rilevare eventuali attività sospette*" spiega **Matteo Rizzi**.

La sicurezza informatica è una responsabilità condivisa

Essere consapevoli delle proprie abitudini online e applicare regolarmente le buone pratiche di cyber-igiene aiuta a prevenire potenziali minacce e proteggere le proprie informazioni e la propria identità digitale.

Il Centro Cybersecurity propone regolarmente iniziative di sensibilizzazione e formazione anche per la community di Fondazione Bruno Kessler. "**How much do you value YOUR privacy"** è stato un evento interno che si è svolto presso l'EIT open space. Durante una dimostrazione dal vivo, con un attacco simulato, i ricercatori del Centro Cybersecurity hanno illustrato quanto i criminali possano raccogliere dai nostri dati personali e hanno spiegato in maniera approfondita alcuni consigli su come proteggere le proprie informazioni online.

LINK

https://magazine.fbk.eu/it/news/ti-prendi-cura-della-tua-cyber-igiene/

TAG

- #cyber-igiene
- #cybersicurezza
- #data breach
- #dataprotection
- #hacker
- #mfa
- #securityandtrust

AUTORI

- Michela Antino