FONDAZIONE BRUNO KESSLER
MAGAZINE

Do you take care of your cyber hygiene?

January 27, 2025

Tips from the Center for Cybersecurity on the Data Protection Day

January 28, 2025 marks **European Data Protection Day**, an important occasion to reflect on the security of personal information online and the importance of adopting appropriate digital protection practices. But what does it mean to take care of your cyber hygiene?

Cyber-hygiene **refers** to the set of practices and behaviors that every user should adopt to protect their digital information and identity online. Just as we take care of our physical health with proper personal hygiene, we should do the same in the digital world to prevent cyber attacks, data theft, and other threats to our privacy.

On Data Protection Day, FBK's Security & Trust Unit researchers and Science Ambassadors **Giada Sciarretta** and **Matteo Rizzi** offer some **practical tips and recommendations for improving your cyber hygiene**. Giada Sciarretta is an expert in design and security analysis of digital identity solutions, Matteo Rizzi is a Security Administrator at FBK with experience in identity management and analysis of security protocols.

Practical tips for cyber-hygiene

Have you ever used one of the most common **passwords** of 2024? According to NordPass, the most commonly used passwords in Italy include combinations of numbers such as 123456 or 12345678, or words such as "password," "cambiami," and "juventus." If you've recognized one among your credentials, it's time to review your online security habits – it's critical to use strong, different passwords for each service.

"Passwords" are the first line of defense against cyber attacks; therefore, it is important to avoid predictable combinations such as '123456' or 'password,' preferring more complex and secure solutions. *A good practice is to adopt a passphrase at least 16 characters long, containing uppercase letters, lowercase letters, numbers and special symbols. Furthermore, it is essential not to reuse the same password for several accounts*," **Giada Sciarretta** said.

Another essential measure is multi-factor **authentication (MFA)**, which adds an extra layer of security by requiring a second factor in addition to the password, such as a code generated by an authentication app or a fingerprint. This greatly reduces the risk of unauthorized access and also

provides greater protection if login credentials are stolen. Seting up MFA for all accounts that support it is one of the best strategies to protect personal data.

Another tip is to use **email aliases**, such as those offered by services like SimpleLogin, which allows you to create temporary aliases to avoid exposing your main address and protect your digital identity. These aliases can be useful for signing up for online services without compromising your main account, reducing the chance of receiving spam or being a victim of phishing. They also provide good protection in case of "**data breaches**," which occur when personal data is exposed or stolen due to a security breach. The main causes of data breaches include hacker attacks, misconfigurations of systems, software vulnerabilities and human negligence. The consequences can be severe, with significant financial and reputational impacts for individuals and companies. To protect yourself, you can check regularly, and see whether your email address has been compromised, on sites such as Have I Been Pwned, change passwords immediately if they have been compromised, and always enable multifactor authentication to limit damage.

"The use of email aliases is also particularly effective in protecting against data breaches: in fact, if one alias is compromised, the user can easily deactivate it without affecting other accounts, thus providing an additional layer of protection. *In addition, the separation between aliases prevents hackers from correlating different digital identities, limiting the possibility of large-scale targeted attacks. Finally, it is a good practice to monitor your accounts frequently and enable login notifications to detect any suspicious activity*,"**Matteo Rizzi** explains.

Cybersecurity is a shared responsibility

Being aware of one's online habits and regularly applying good cyber hygiene practices helps prevent potential threats and protect your information and digital identity.

The Center for Cybersecurity regularly offers awareness and training initiatives for the Fondazione Bruno Kessler community. '**How much do you value YOUR privacy'** was an internal event that took place at the EIT open space. During a live demonstration with a simulated attack, researchers from the Cybersecurity Centre illustrated how much criminals can collect from our personal data and explained in depth some tips on how to protect one's online information.

PERMALINK

https://magazine.fbk.eu/en/news/do-you-take-care-of-your-cyber-hygiene/

TAGS

- #cyber hygiene
- #cyber-igiene
- #cybersecurity
- #data breach
- #dataprotection
- #hacker

- #mfa
- #securityandtrust

AUTHORS

- Michela Antino