SAFE ON SOCIAL
TRAINING AND EDUCATION

Encryption Explained

www.safeonsocial.com

Encryption explained.

Encryption is an invisible safety net for our data, but its role is a hot topic of conversation worldwide in government debates again. Understanding the tech we use every day is super important. Why? The world of tech changes so quickly that it's hard for laws and rules to keep up. So as the debates and slow-moving safety by-design strategies continue for what will no doubt be more and more years, abhorrent behaviour and breaches in security online continues.

Continual learning is crucial. There's an old saying that the only constants in life are death and taxes. Perhaps we should now add rapid technological advancement to that list. Technology often outpaces laws and regulations, with many tech companies prioritising profits over people's wellbeing.

Before founding Safe on Social 14 years ago, I spent nearly two decades working in cybersecurity, a field I loved and still do. Given that I wasn't particularly fond of mathematics during my school years, it was quite ironic that a substantial part of my work involved encryption, a complex area heavily reliant on mathematical principles.

The core of my work was bridging the gap between highly technical teams and end users, who were typically governments and businesses. This role as a translator remains central to my work at Safe on Social today. It's crucial for us as individuals to educate ourselves, and our children, about navigating the online world safely and intelligently.

Understanding encryption, what it is, how it functions, and why it's vital forms a significant part of this education.

Encryption is a largely invisible security guard online. It converts standard information into an unreadable format, much like a sophisticated version of a secret language or code. Just as a decoder can decipher a secret code, a decryption key can unlock encrypted data and return it to its original format.

So this is the very basics of how end-to-end encryption, one of the most secure types of encryption works. We all use it everyday but you can see it. If you could see it magine two people, Jaclyn and Rikki, wanting to share a secret message. Jaclyn writes a note and locks it in a box using a padlock. She then sends the locked box to Rikki. Now, only Rikki can unlock the padlock, as she is the only one with the key. In this scenario, the note represents the email message, the locked box is the encryption, and Rikki's key is the decryption key. Even if someone else intercepts the box during its journey, they cannot open it without the key.

So why is encryption so crucial? It enhances privacy and
confidentiality. Encryption is like sending a letter in a tamper-proof envelope that only your intended recipient can open. This becomes especially important when handling sensitive personal data such as social security numbers, bank account details, and private conversations.

Encryption plays a dual role in authentication and integrity. Think of authentication as getting a text message from a friend. Your phone shows their name because it recognises their number, just like encryption confirms the identity of the sender. Meanwhile, integrity is like receiving a snap on Snapchat. You're the first and only person to see it when you open it. If someone else had opened it, you'd know because the app would tell you. This is how encryption ensures a message hasn't been interfered with during its journey.

The level of security encryption provides is dependent on the complexity and length of the encryption key, as well as the encryption type used. More complex keys create a stronger lock that is harder for anyone to pick.

Encryption is a silent aspect of our day, working in the background without our active awareness. When you browse a website whose address begins with 'https', it is a secure connection. The 's' stands for 'secure', indicating that the data transferred between your browser and the site is encrypted. This silent operation protects your information from potential unauthorised access.

When sending emails via secure platforms, encryption acts like a protective envelope around your messages, ensuring their privacy. Messaging apps like WhatsApp and Signal also employ encryption technology, safeguarding your conversations from potential breaches.

Encryption plays a crucial role in online banking and shopping transactions. It acts as a vigilant security guard, keeping your sensitive financial details secure when you check your account balance, make transfers, or shop online. Encryption is continually operating behind the scenes to protect your online activities.

Password managers are another everyday example of encryption in action. These tools store passwords in an encrypted format, making them accessible only via a master password known only to the user. In this way, even if the password manager's database was compromised, hackers would only find a collection of encrypted passwords, which would be useless.

While many password managers offer premium versions, free versions can also provide adequate security for the average user. Among these, Apple's Keychain is a popular choice for Apple users, as it is built into iOS, macOS, and Safari, providing seamless integration and ease of use.

Apple Keychain securely stores passwords and credit card information, and it can auto-fill these on websites and apps across your Apple devices. It employs end-to-end encryption, ensuring that only you can access your data. Furthermore, as it's part of the Apple ecosystem, it is continuously updated and maintained, providing a level of trust and reliability. Apple Keychain's effectiveness is mostly limited to the Apple ecosystem, which can be restrictive if you use devices from different manufacturers or prefer other browsers to Safari.

Google's own Smart Lock feature is built into every Android device and offers similar functionality. Like Apple's Keychain, Google Smart Lock can save and auto-fill passwords across Android devices and Chrome browsers.

There are also many third-party password managers that are compatible with both Android and Apple platforms, such as LastPass, Dashlane, and Bitwarden. These services offer apps for Android, iOS, Windows, macOS, and most web browsers, allowing you to access and sync your passwords across multiple devices, regardless of their operating system.