TERRANOVA SECURITY

TERRANOVASECURITY.COM

7 END USER DATA PRIVACY AWARENESS TIPS

1

Understand what constitutes personal information

Personal information refers to any data elements that, alone or in combination, can be used to identify an individual. These can include (but is not limited to) your email address, phone number, passport or driver's license number, medical or financial documentation, IP addresses, fingerprint data, and much more. Terranova Security recommends sharing this type of information only when necessary and solely with trusted recipients or organizations that demonstrate acceptable data privacy practices.

2

Use secure Wi-Fi networks, a VPN

To minimize the possibility of data exposure, avoid entering personal information, including your credit card number or address, over a public Wi-Fi network. Instead, use password-protected internet access points and, whenever possible, a personal Virtual Private Network (VPN) for additional security.

3

Verify the legitimacy of a website URL

Before sharing any personal information online, verify the web address's legitimacy. Ensure that "https://" is part of the domain or that a closed padlock is visible next to your browser's address bar. Even for secured sites, Terranova Security recommends enabling two-factor authentication for your online accounts, especially for e-commerce.

4

Beware of phishing attempts

Cyber criminals engineer phishing email scams to steal personal user data and use it to commit identity theft or other malicious activity. It is vital to be vigilant at all times and never share personal information via email unless you're sure of the recipient's identity and how that data will be handled and stored.

5

Be mindful of other cyber threats

Phishing is not the only threat that can compromise a user's data privacy. Be on the lookout for other forms of social engineering, such as smishing (phishing via SMS messages) and vishing (voice messages). These fraudulent, urgent-sounding communications often appear to come from familiar sources and often unsolicited. If uncertain, hang up and call official numbers directly.

6

Report suspicious requests for information

Spam email filters and other technical precautions won't automatically ensure that your data's privacy is upheld. If you notice any suspicious messages or activity you believe may have compromised personal information, report it to your IT department or the proper authorities immediately.

7

Embrace security awareness training

Data privacy best practices must be observed by organizations and individuals that handle the personal data of others.To fully protect all information, everyone should embrace and complete at least one form of security awareness training. You'll gain the knowledge you need to keep your data secure and also create and strengthen good online habits.

TERRANOVA SECURITY