VIALET

ENHANCING YOUR SECURITY AWARENESS: PROTECT YOUR DATA AND DEVICES

At VIALET, your security is our top priority. We want to ensure you have the knowledge and tools to protect your personal information, accounts, and devices while using our services. As part of our ongoing customer education and awareness initiative, we are sharing some essential security practices to help you stay safe online.

Protect Your Personal Data and Account Information

To keep your account secure, it is crucial to protect the following:

- **Passwords and PINs**: Always create strong, unique passwords for each account and never share them with anyone.
- **Security Tokens**: Keep your tokens (such as two-factor authentication devices) safe and secure. If lost or stolen, report them to us immediately.
- **Personal Details**: Be cautious when sharing sensitive information like your personal ID, Social Security number, or account details. Only provide these to trusted sources and be aware of phishing attempts.
- **Confidential Data**: Always handle your financial and account information with care, and avoid storing it in easily accessible locations, such as your mobile notes or public cloud services.

Safeguard Your Devices

Properly managing the security of your personal devices - whether it's your computer, mobile phone, or tablet - is essential for preventing unauthorized access to your account. Here's how:

- **Install Antivirus Software**: Ensure that you have a reliable antivirus program installed on your devices to detect and block malicious software.
- **Update Security Patches and Firewalls**: Regularly update your device's operating system, apps, and security features. This includes installing the latest security patches and enabling firewalls to protect against vulnerabilities.
- **Avoid Unsecured Wi-Fi**: When accessing your account or making payments, avoid using public or unsecured Wi-Fi networks. Use a secure, private connection instead.

Be Aware of Downloading Risks

Downloading software from the internet can pose significant threats to your device and personal data if you're not cautious. Here are some best practices:

- **Verify Software Authenticity**: Only download software from trusted sources and official websites. Be wary of third-party sites or downloads that seem too good to be true.
- **Check for Tampering**: Ensure that any downloaded software has not been tampered with or modified. Use checksums or other verification methods when available.
- **Avoid Suspicious Links and Attachments**: Never download software from unsolicited emails or links. These could contain malware designed to steal your personal information or damage your device.

Always Use Our Genuine Platforms

When accessing your VIALET account or making transactions, it's essential to use only our **official website or mobile app** to avoid phishing scams or counterfeit sites. Here's what to keep in mind:

- **Access the Genuine Website**: Always type in our official URL directly into your browser (e.g., www.vialet.eu) and avoid clicking on links in unsolicited emails or messages.
- **Use the Official Mobile App**: Download our app from trusted sources like the Apple App Store or Google Play Store. Regularly update it to ensure you have the latest security features.
- **Beware of Phishing Scams**: If you receive emails or messages claiming to be from VIALET asking for personal information or payment details, be cautious. Verify with us directly if the request is legitimate.

Stay Informed

As part of our ongoing commitment to your safety, we will continue to share security updates and tips through our customer education programs. Please feel free to reach out to us if you have any questions or concerns.

By following these security measures, you'll help protect your account and personal information from potential threats.

Thank you for taking the time to keep your online activity safe and secure.