Vialok Security Best Practices

Congratulations! You've taken the most effective step toward securing your personal information and the highly sensitive information of your clients by using the Vialok security platform! The Vialok platform is a form of multifactor authentication—considered by cyber security experts to be one of the most important and effective methods of securing personal data.

When using Vialok to verify settlement instructions, you can be assured that you've taken the strongest line of defense against wire fraud.

By now you've experienced the ease of using the Vialok platform and know how seamlessly it integrates into your daily routine. And even though simply using the platform dramatically enhances the security of highly sensitive settlement information, implementing security best practices in all aspects of your daily business routine will improve your security overall.

But first, a little bit about optimizing your use of the Vialok platform…

Vialok Security Best Practices

Specifically For Client Administrators

1. **Use Vialok with Fidelity** Require that all parties involved in the closing process always use Vialok to confirm any changes to settlement instructions. If Vialok is not used with fidelity, the security of your settlement information may be compromised.

2. **Registration Codes** When you add new Contacts to a File, Vialok will automatically generate a Registration Code. The most secure way to provide your users with this information is over the phone or in-person.

3. **Expiration Windows** Client administrators will have the option of setting the expiration window for the registration codes generated by Vialok for each Contact and for messages created and sent through the Vialok platform. We suggest an expiration window of less than 24 hours.

4. **Compromised Devices** Client administrators will also be able to select whether to enable the registration of jailbroken or rooted devices. By default, the Vialok platform will deny registration to these altered devices since they are inherently less secure.

For All Users

1. **Selecting a PIN Code** All users will be required to select a numeric PIN Code upon registration. PIN Codes must be between 4-36 digits long. We suggest choosing a PIN Code that is at least 6 digits long (the longer the PIN, the higher the level of security). Also, avoid using personal information for your PIN Code (for example: your birthdate, the birthdate of a close relative, your social security number-- anything that can be

guessed with just a bit of digging into your background).

2. **Storing your PIN Code** Protect the security of your PIN Code like you would your ATM pin. Do not store your PIN Code on your mobile device or attach it to your desktop computer with a post-it note. Do not allow your internet browser to store your PIN. This is a convenient feature, but it leaves one factor of authentication vulnerable if someone obtains access to your device. If you have trouble remembering your PIN, save it in an encrypted text file or use a password manager software.

General Security Best Practices

For Management

1. **Office Policies and Procedures** The most important step in ensuring the security of your business is to create clear policies and procedures that are implemented office-wide. These policies and procedures should cover the security issues often present in your business, such as logging out of programs and locking computers when away from your desk, what to do if you receive a suspicious email, and rules on using public Wi-Fi for office-related activities. Of course, the most important policy is to always use Vialok when confirming or denying settlement instructions. Some of the most common policies and procedures will be discussed under 'For All Employees.'

2. **Training Employees** Once your policies and procedures are in place, use the documentation to train your employees. Provide regular refreshers—adding to your policies and procedures as new security issues arise. Make sure that everyone working for your company is trained and adheres to these guidelines, from the CEO to contractors and temporary workers. After all, security policies and procedures are only effective if they are implemented correctly and consistently!

3. **A Multi-Antivirus Approach**: With new threats being introduced daily, it's important to use multiple antivirus engines in order to increase the rate of detection and reduce the window of vulnerability. We recommend that *every* business use a host-based intrusion detection system and that larger companies *also* use a network-based intrusion detection system.

   Further, since email is one of the main sources of malware, you may want to use a high-performance email antivirus to scan incoming email attachments for email-borne threats. Malware is usually found in emails coming from external sources, but if an employee's machine gets infected, malicious emails can be sent via internal email. Employees are also more likely to click on an infected email attachment if it's from a co-worker. For this reason, it's important to ensure that your email security solution also scans internally sent emails.

For All Employees

1. **Public Wi-Fi:** Hackers are known to intercept the information sent through legitimate public Wi-Fi networks or they trick your mobile device into using their Wi-Fi hot spot, enabling them to view and modify your traffic. Vialok is not susceptible to these sorts of attacks, but your other communication channels may not be as secure. Therefore, avoid sending unencrypted, personal information over public Wi-Fi, and check your mobile device settings so that your cell phone does not automatically connect to local Wi-Fi networks.

2. **Site Credentials:** Check the website's SSL certificate before sending personal information over the internet. Whereas "https" offers a level of security, a URL with only "http" is NOT secure. Navigate unsecured sites with caution.

3. **Mobile Communication**: Only use secure communication channels to send sensitive information. Vialok can detect whether a device has been compromised (through cloning, malware, etc.) and can authenticate registered parties. Without Vialok, you can't be certain who you're communicating with.

4. **Lock Screens** When you're in a private space, always lock your computer or mobile device when you leave them unattended for short periods of time. Avoid leaving your devices unattended in public places.

Email Best Practices

1. **Spam and Phishing Emails**: Spam is not only a nuisance-- it can also pose security risks. Phishing emails entice recipients to click on malicious links to steal credentials or confidential information. Use your spam filter to isolate any suspicious content. If an email looks suspicious, or if you don't know the sender, avoid replying or responding to requests. If the sender is legitimate, they'll probably provide an alternate form of communication. A simple phone call to confirm the sender's identity will save you the trouble of a security breach.

2. **Confidential Content**: Only use secure platforms to send confidential content. The Vialok platform enables documents to be sent and viewed securely; only use the Vialok platform to send closing documents that require confirmation.

3. **Attachment Awareness**: Don't open any attachments from unknown senders. If the attachment prompts you to enable features or connect to the internet, close the attachment immediately and report it based on your company's security policy.