Securing the Merchant's Site That Uses i4Go

Take these steps to ensure your website is secure before going live with Shift4's i4Go®:

1. Password Hardening
2. Software Patching
3. Network Security
4. User Security

Note: i4Go is designed to secure cardholder data (CHD) in eCommerce business environments with web browser-based applications that integrate online (website) and onsite (kiosk, Software as a Service) technologies by intercepting CHD at the point of entry — before it ever enters the merchant's Web server or hosting provider's system — and working with Shift4's PA-DSS validated Universal Transaction Gateway® (UTG®) or API Web service and PCI DSS-compliant Lighthouse Transaction Manager payment gateway to replace the CHD with a payment token, a unique ID to reference the actual data. This will drastically reduce eCommerce merchants' PCI DSS scope and may qualify them to use the SAQ-A (EP).

Step 1: Password Hardening

Use two-factor authentication for all administrative logins to your website and network systems.

Important: Completing this step is critical.

- Find a third-party app for two-factor authentication (2FA) to the website's administrative panel and sensitive settings. (Authy, Microsoft, Google, and LastPass Authenticators are a few of the top software solutions for 2FA.)
- Human made passwords should use a "passphrase" creation strategy. Longer length increases its strength. To build a passphrase, use four words not commonly found next to each other to create a password. Non-letter characters can be added to increase complexity, if desired. For example: dinerfighteat1@night.
- Don't reuse or share passwords for other accounts. Every account needs its own unique password that is stored securely.
- Use a password manager for secure storage. (Lastpass, Keepass, Roboform, 1Password, and Dashlane are a few suggestions, but there are many choices. Look at features to find the one that is best for your business needs.)
- Every default password needs to be changed prior to a device or software being used in operations.

WARNING! All default passwords can be found using Google Search which is why it is critical they are changed to unique passwords.

- Do not allow common password templates (e.g., Winter2019!). Avoiding dangerous templates can be accomplished by setting your password minimum length to 18 characters and asking employees to create a passphrase.
- Securely store password backups as directed by your password manager.

Step 2: Software Patching

All software needs to be patched at some point in its lifecycle. (There may be exceptions, but there are few.)

- Use the automatic updating feature on all software installations that provide it. If you are unsure, search Google for "how to update [app name]." For example, "How to update Firefox?"
- Only use updates installed automatically from within the application or downloaded from the device or software manufacturer directly.
- Software vendors provide "security advisories" on their websites to alert customers of new updates. Subscribe to the security advisories on vendor websites for all devices and software utilized.
- The older a security issue is, the bigger the risk that someone is targeting the issue. Apply patches in a timely manner. Generally speaking, 30 days is a good target timeframe for patching from a patch release.
- Make a note about any vendor that does not deliver security advisories to you automatically, and plan to check their website for updates periodically.
- Only perform updates while connected to your secure network or another trusted network.
- Do not install anything that comes in an email attachment. Go to the vendor website and download it.
- Use Google, or another search engine, to find the vendor websites to download from. Do not click on advertisements or links from emails.
- Uninstall all End of Life (EOL) software. To find EOL dates, search Google for "EOL [app name & version]." For example, "EOL Winzip 20.5." EOL software is no longer being updated, and issues are not being fixed.

Step 3: Network Security

The network infrastructure for your commercial networks should be configured by a qualified individual.

- Proper network segmentation will reduce impact of any infections on the network to a limited scope.
- Proper network segregation will obscure sensitive transactions from other network traffic.
- Segregate network management traffic from normal network traffic.
- Use VLANS to give different types of traffic dedicated subnets.
- Disable unwanted or insecure features, protocols, services, and ports on network equipment.
- Restrict remote administrative access to networking equipment using IP filters, 2FA, and access control lists.
- Change default settings on networking devices to harden your infrastructure.
- Keep access to network equipment secured inside a locked cabinet.
- Use Windows firewalls and Network firewalls. Use an antivirus on every computer.

- Back up configuration files for networking gear, and store them offline. Protect Config files with encryption when sending, storing, or backing up.
- Prioritize using systems that can assign different privilege levels for various accounts.
- Monitor and review network logs. Also, forward all logs to a secure server.
- Inspect devices connected to the network for signs of tampering, and validate serial numbers for devices.

Step 4: User Security

User actions can result in network infections of all types. Here are steps to take to reduce exposure to this threat.

- Limit internet access for employees to devices that do not perform business functions.
- Lock down business computer systems so they only perform their primary business functions.
- Do not share any computer related accounts between users. Each person needs their own account.
- If providing customer access to the internet, do so on a segregated network that uses a separate access point, a captive portal, is encrypted, and is password protected.
- Teach employees to discard unsolicited emails with attachments, and scan all email attachments using an antivirus before opening.
- Use an antivirus on every computer on your network.
- Use a VPN if providing remote access to your network, and only provide remote access to trusted employees and third parties. Disable their access when it is not needed.
- Disable Macros in Microsoft Office documents to help prevent the execution of ransomware and other malware on your network.