SLASHNEXT

Mobile Security Technical TOI

Smishing & multi-channel phishing protection for iOS & Android

Jimmy & Vamsi

Product Management

July 15, 2022

Lasted updated Jan 19, 2023

Agenda

1. Mobile Security Business
2. Mobile Security Personal
3. Smishing & Real-time Click Protection FAQs
4. FAQ Cheat sheet
5. Voucher Portal & FAQs

Mobile Security Product Portfolio

- Mobile Security **Business**
  - Incidents and device status recorded to CMS
  - Deploy using UEMs or invitation email with activation key
- Mobile Security **Personal**
  - Only device status recorded in CMS
  - Deploy using Intune UEM or invitation email with activation key
- Mobile Security **Home**
  - No information record in CMS
  - Download from app store
  - Activate by using voucher code or in app store purchase

SlashNext Mobile Security Business

Summary of features and concerns

Features

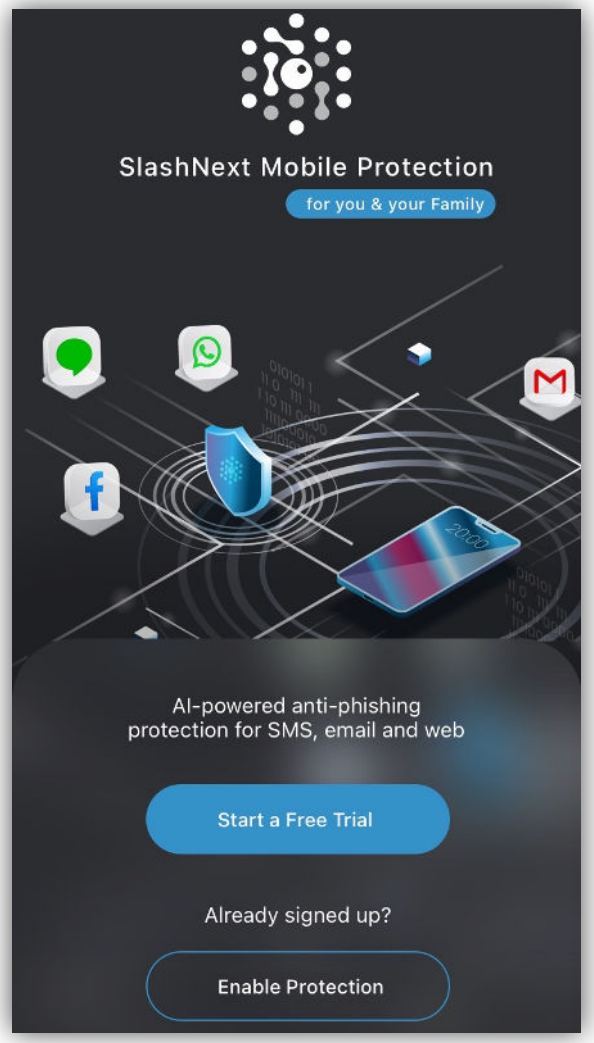
- Business Text Compromise (BTC-ing) and link-based smishing protection
- Real-time click-time protection in any app
- Centrally managed, multiple deployment options, incidents written to CMS, and supports all device types: supervised, managed BYOD and unmanaged “personal” BYOD

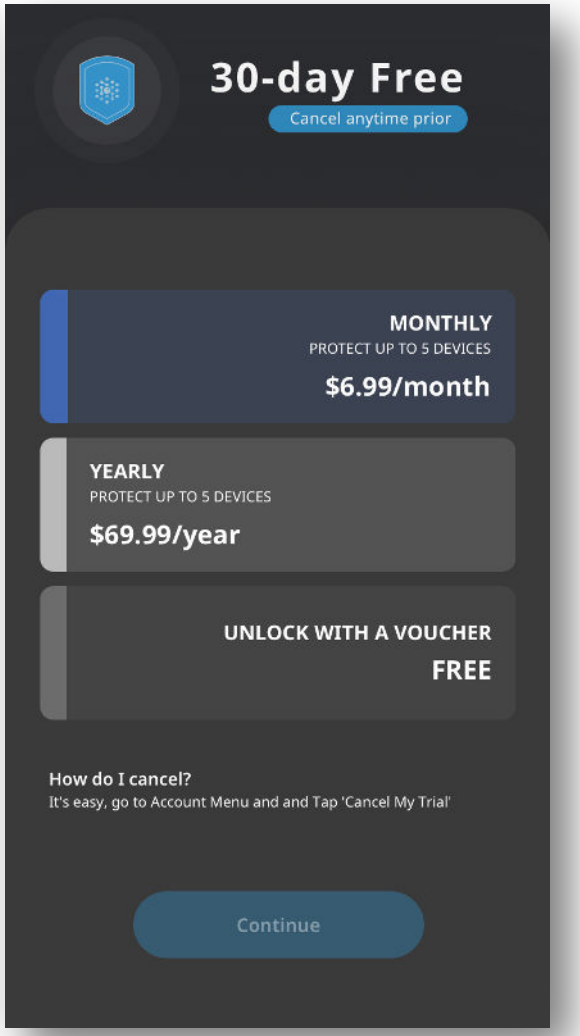
Concerns

- **User privacy for BYOD -** “…employees are tired of us shoving security down their throats” – M&N
- Deployment and operational cost

SlashNext Mobile Security Personal

Smishing & multi-channel phishing protection for personal BYOD





COMPLETE PRIVACY	No user & incident details are collected. Threat analysis performed on user device
VOLUNTARY INSTALL	User download from app store and activate using voucher code. Maintenance free
FAMILY SHARING	Protect family members with support for up to five iOS and Android devices
SMS PROTECTION	Stop Business Text Compromise and link-based Smishing attacks using on-device NLP ML & AI intelligence DB
WEB PROTECTION	Block access to phishing webpages across all apps and channels, and against all phishing payloads

SLASHNEXT

Device Operating Modes

OS	Operating Modes and Profiles	MDM Managed?	Restriction Level
Apple iOS	Supervised	YES	HIGH Managed apps only
	Managed BYOD	YES	MED Managed and Unmanaged/Personal apps
	Unmanaged “Personal” BYOD	NO	LOW Unmanaged apps
Google Android	Work Profile	YES	HIGH Managed apps only
	Personal Profile	NO	LOW Unmanaged apps

Mobile Security Protection Matrix

Updated 2/17/23

For Devices Already Installed with VPNs

Mobile Security

Mobile Security Protection Matrix

Mobile Device Mode	SMS Protection	Web Protection
iOS supervised	Yes	Yes
iOS non-supervised	Yes	No
Android	Yes	No

SLASHNEXT

Mobile Security Cheat sheet

OS	Operating Mode and Profiles	Works with other VPNs	SMSing Protection - Attributes analyzed[1]	SMSing Protection - Exception	Real-time Click Protection	Compatible w/ Business, Personal & Home
Apple iOS	Supervised	YES	Text + Normal domains + Shared domains	iMessages From contacts From short numbers From toll free numbers Have conversation history	Blocks clicks to Shared domains + Normal domains + URL shorteners	YES
	Managed BYOD	NO	Text + Normal domains	Same as above	Blocks clicks to Normal domains + URL shorteners	YES
	Unmanaged BYOD/ ”Personal” BYOD	NO	Text + Normal domains	Same as above	Blocks clicks to Normal domains + URL shorteners	YES
Google Android	Work Profile	NO	Text + Normal domains	From short numbers From toll free numbers	Blocks clicks to Normal domains + URL shorteners	YES
	Personal Profile	NO	Text + Normal domains	From short numbers From toll free numbers	Blocks clicks to Normal domains + URL shorteners	YES

1 - URL shorteners, i.e https:bit.ly/3el, are not listed in on-device DB

SLASHNEXT

Smishing Protection FAQs (1/3)

How do you protect my privacy?

- Nothing leaves the device. Analysis is performed on the device
- SlashNext Mobile Security Personal - No tracking/reporting/recording
- SlashNext Mobile Security Home - No tracking/reporting/recording
- SlashNext Mobile Security Business - Only incidents are recorded in Cloud Manager for reporting and IR

What is recorded in Cloud Manager for Mobile Security Business

- iOS – Nothing
- Android – Entire smishing message

What is my user experience?

- iOS – Smishing messages are moved to Junk Folder
- Android – User is alerted when Smishing messages are received

Smishing Protection FAQs (2/3)

How Does it Work?

1. Text is checked by on-device NLP ML + Domain is checked by on-device AI phishing intelligence database
2. Text message is classified as smishing if any of the two detection techniques returns a malicious verdict

Which type of domains are checked for Smishing protection?

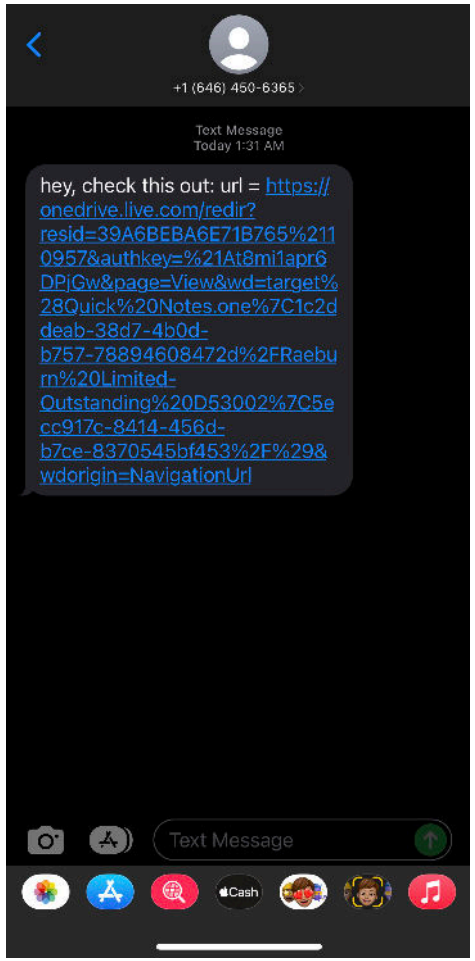
- iOS Supervised mode – Normal and shared domains
- iOS Managed and Unmanaged mode – Normal domains
- Android – Normal domains

What are the 3 types of domains?

- Normal Domains: https://cnn.com
- Shared Domains: https://sharepoint.com, https://wix.com
- Shortener/Redirectors Domains: https://bit.ly

Shared Domain Behavior Explained

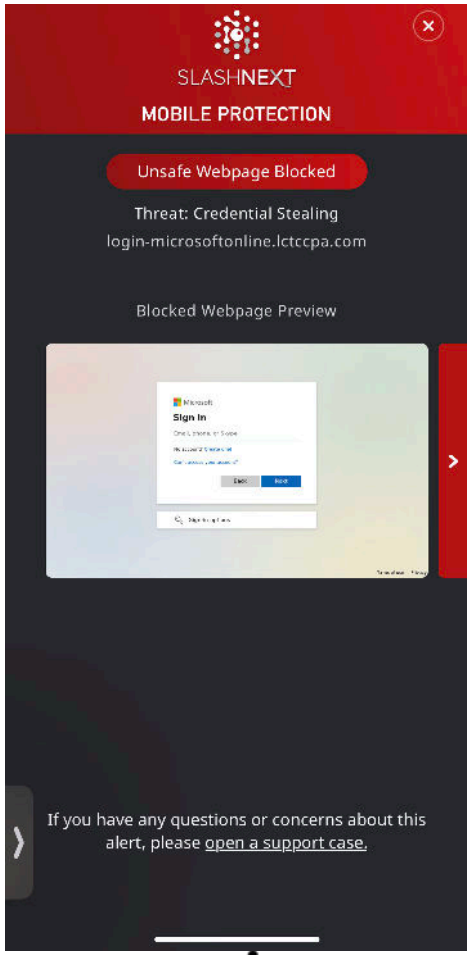
1 Text, and URL on shared domain onedrive.live.com did not trigger detection. Msg arrives in Messages folder



2 Click-time protection did not block access to “intermediary” URL on shared domain onedrive.live.com

3 Click-time protection block access to final URL

https://**login-microsoftonline.lctccpa.com**



SLASHNEXT

Smishing Protection FAQs (3/3)

Are there any exclusions from Smishing protection

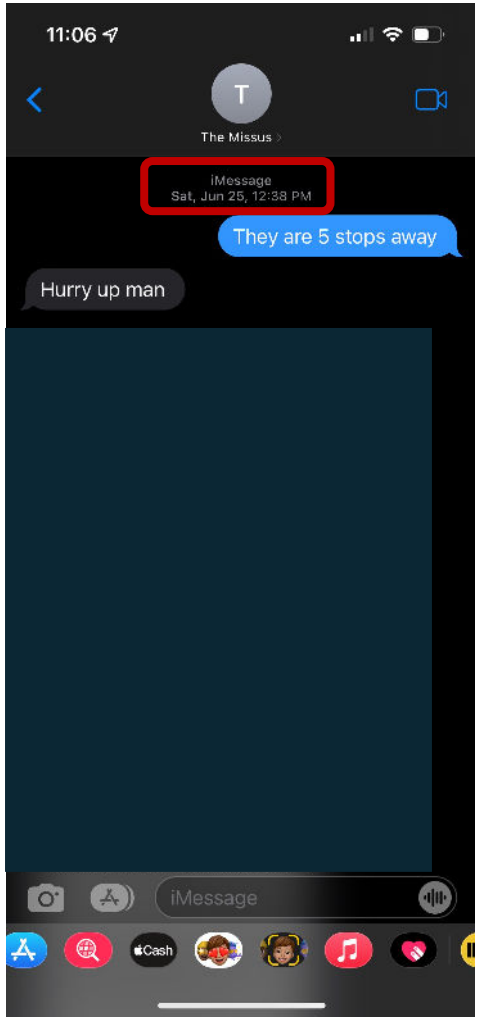
Exclusions mitigates the risk of false positives

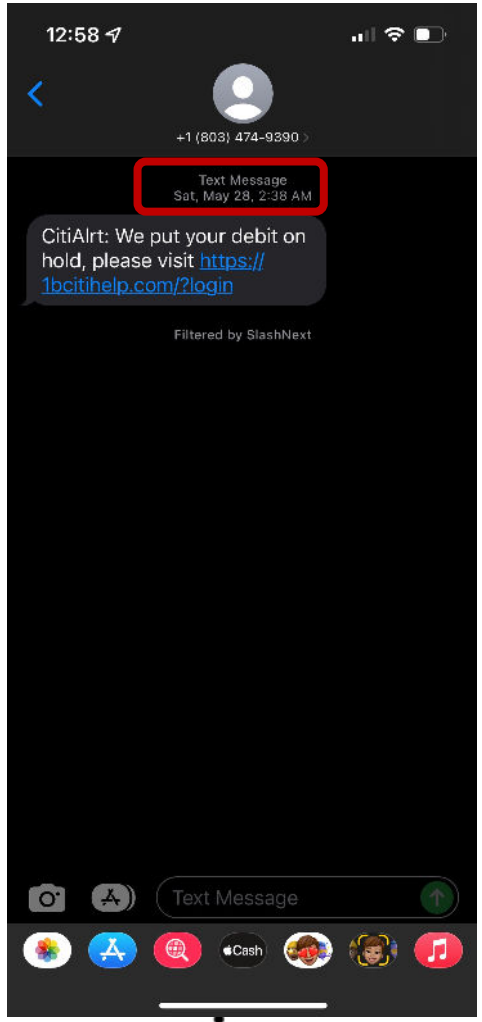
iOS only

- iMessages - iMessage and text banner indicates on how the message was received on the target device
- From contacts
- Have conversation history (3)

iOS and Android

- From short numbers such as “7535” owned by AT&T
- From toll free numbers, i.e. 800





Real-time Click Protection FAQs

How Does it Work?

1. At time of click, from any app, Mobile Security app “sees” the DNS request of the target domain
2. The domain is checked against the list of phishing domain in the on-device AI phishing intelligence database
3. If the domain is listed -> access to URL blocked, user sees an alert banner, with options to view a screenshot and description of the blocked webpage

Why doesn’t work on devices with apps using VPN, i.e. Express VPN?

- Mobile Security app installs a “local” VPN, and a device can use only one VPN at a time
- iOS Supervised mode is compatible on devices with apps using VPN

Are there better alternatives to “local” VPN architecture?

Local VPN is the best architecture. Other architecture has major drawbacks:

- Only protect against webpages opened in Safari app
- Doesn’t protect against phishing webpages opened in Google, Chrome, and other web browser apps
- Doesn’t protect against phishing webpages opened in in-app browsers, i.e. twitter, facebook, WeChat

Other FAQs

When admin install current mobile app, via MDM on Work profile, will it protect users against attacks on Personal Profile?

- NO, when admin install app on Work profile, it will protect only Work profile. Admin can’t deploy an app on Personal Profile using MDM. User has to install an app from google play store manually.

If "no" to q1 Can admin install current app on work profile and install current app again on personal profile via MDM

- Admin can’t deploy an app on Personal Profile using MDM. User has to install an app from google play store manually.

Can admin push current app to work profile via MDM and user install personal app to personal profile via App Store?

- Correct.

Can admins deploy Personal Mobile Protection using UEMs? I know it doesn’t make sense for companies to want to do this but I want to know the answer in case it gets asked.

- Yes, Admin can install any Personal Mobile Protection using UEM but if an app contains any activation process/ licensing model, it will not be auto activated.

Quiz Time!!!

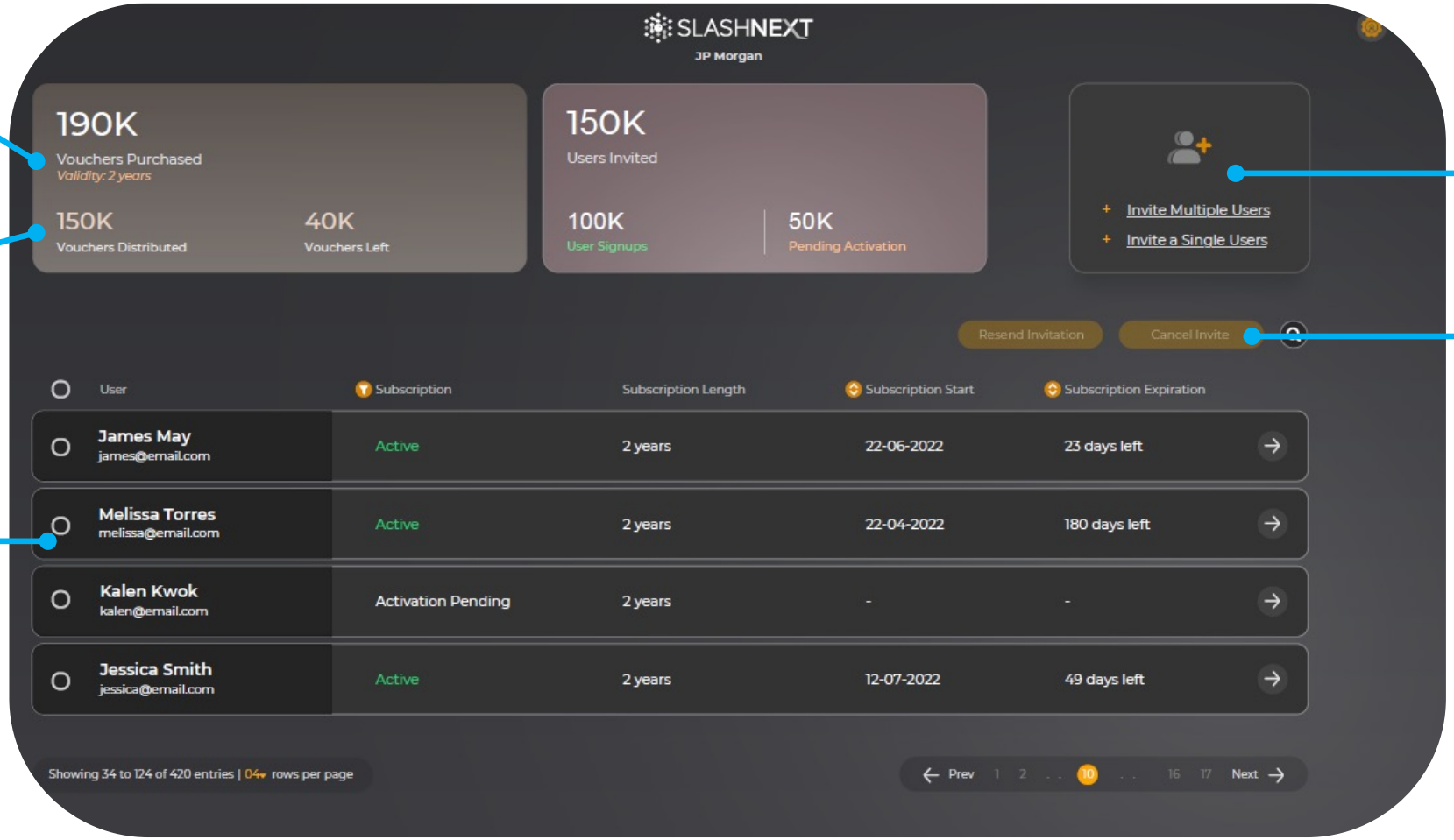
OS	Operating Mode and Profiles	Works with other VPNs	SMSing Protection - Attributes analyzed[1]	SMSing Protection - Exceptions	Real-time Click Protection	Compatible w/ Business and Personal
Apple iOS	Supervised					
	Managed BYOD					
	Unmanaged BYOD/ ”Personal” BYOD					
Google Android	Work Profile					
	Personal Profile					

1 - URL shorteners, i.e https:bit.ly/3el, are not listed in on-device DB

SLASHNEXT

Mobile Security Personal Customer Portal

Key features



Entitlement

Usage

Employee subscription info

Create & send voucher

Available actions

Mockup file here

SLASHNEXT

Voucher FAQs

- What are details captured for every activation?

✓ Name & email of primary user

✓ Subscription start & end date

✓ Number of devices activated

- What happens to protection when an employee leave a company?

✓ Protection will continue to work until Voucher expires.

- What happens to voucher distributed and not activated by end user?

✓ Enterprise can cancel invite and re-distribute the voucher to different user.

Resources

- TOI folder here
- Mockup folder here

Thank You

SlashNext Mobile

Simple, safe and secure

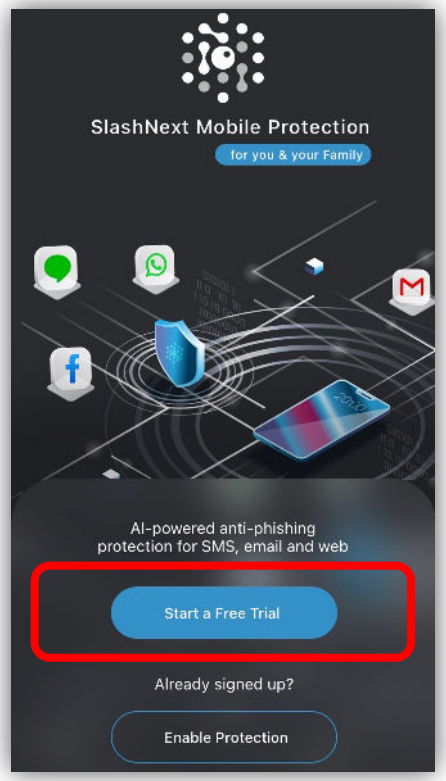
Image for securing all device types

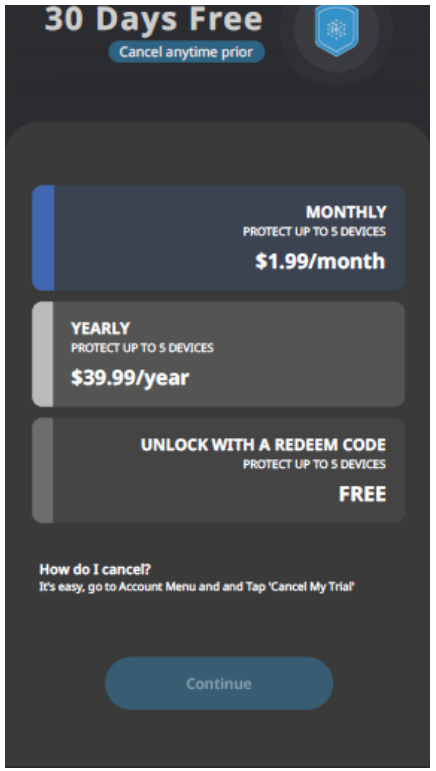
MULTI-DEPLOYMENT OPTIONS	Available for Personal, Managed, and Supervised iOS and Android smart phones and tablets
PERSONAL MOBILE PROTECTION	No tracking. No IT overhead. User install from app store using voucher code for up to 5 devices
BTC PROTECTION	Stop Business Text Compromise and link-based Smishing attacks using on-device NLP ML & AI intelligence DB
TIME-OF-CLICK PROTECTION	Block access to phishing webpages across all apps and channels, and against all phishing payloads
ENTERPRISE USER EXPERIENCE	Safe preview of phishing webpage with threat description to reinforce user awareness training programs

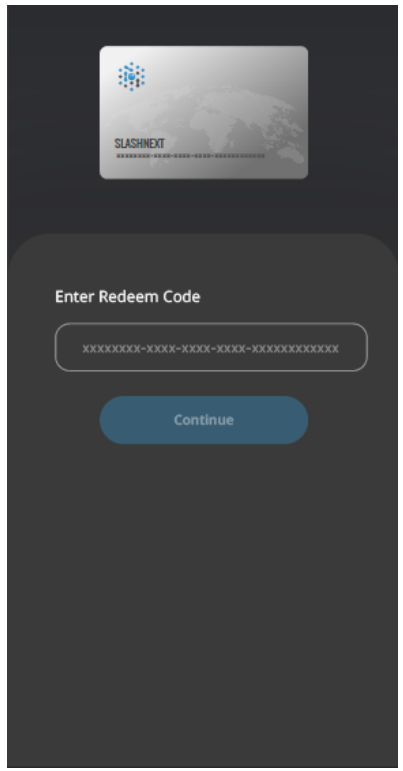
SLASHNEXT

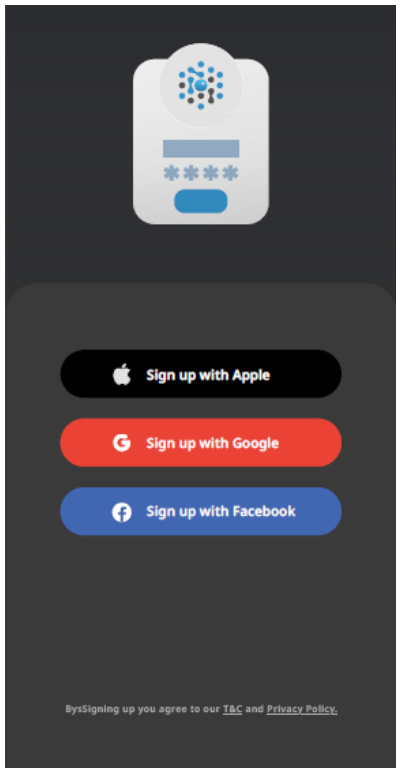
Purchase and Activation

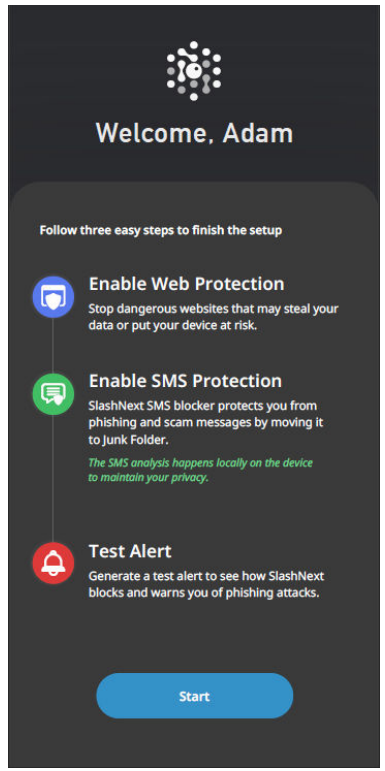
New user making initial purchase using free voucher







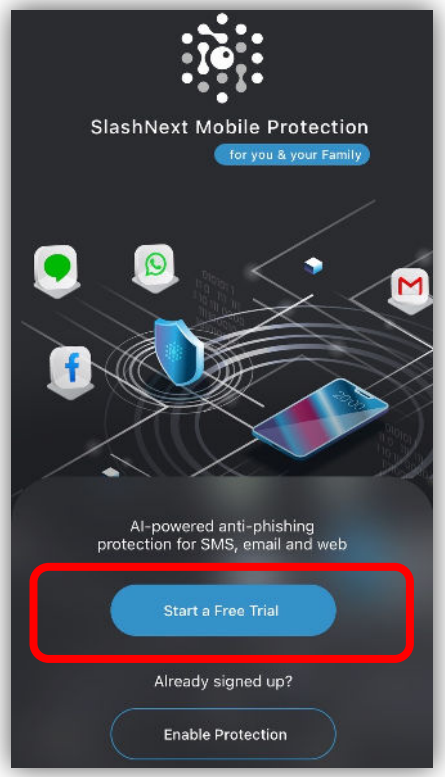


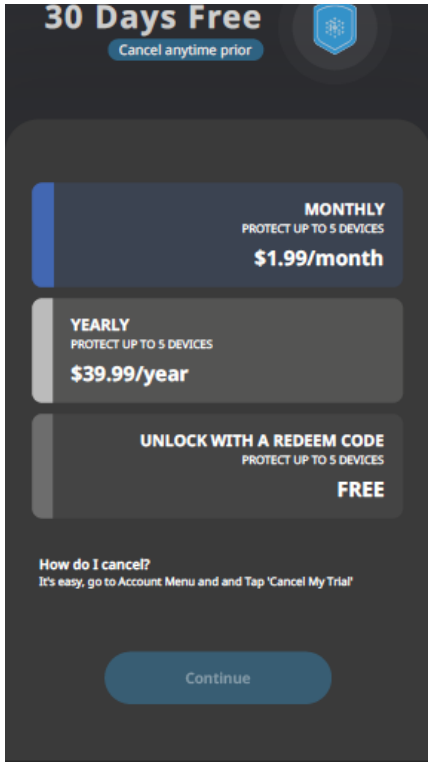


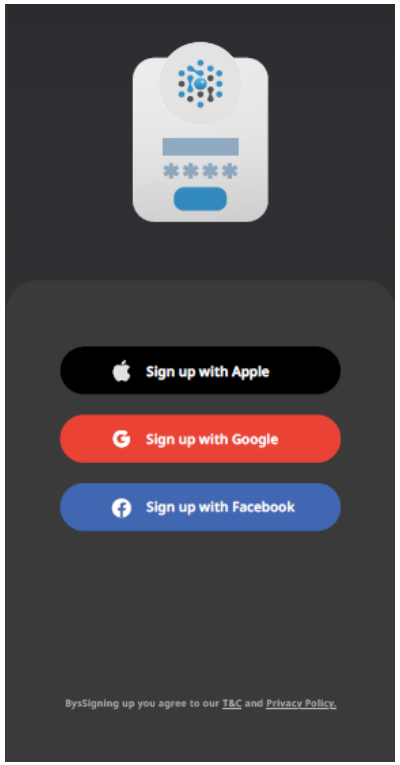
SLASHNEXT

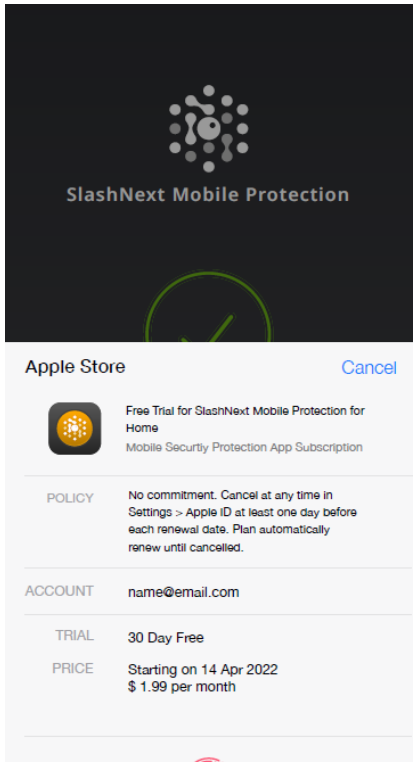
Purchase and Activation

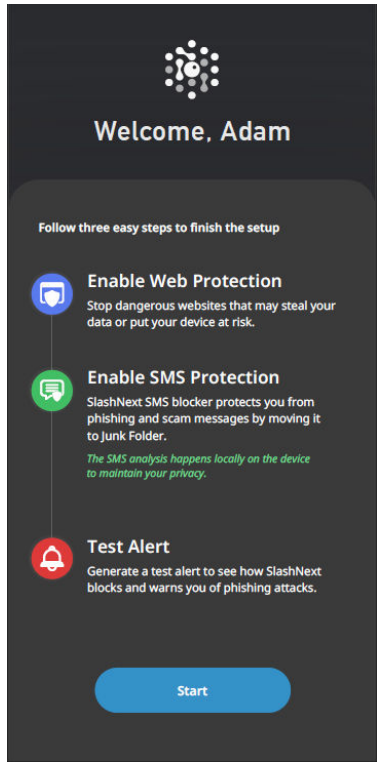
New user making initial purchase using in-app purchase feature







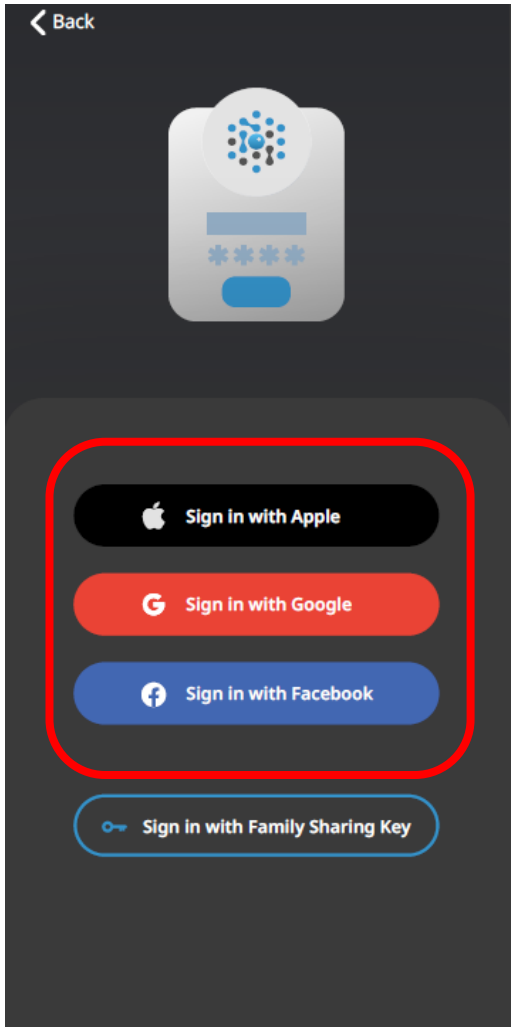


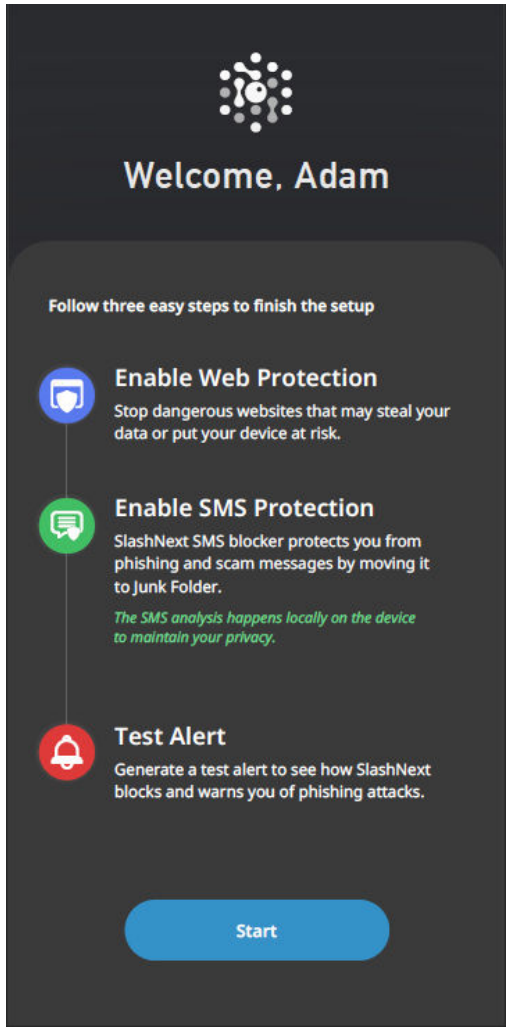


SLASHNEXT

Purchase and Activation

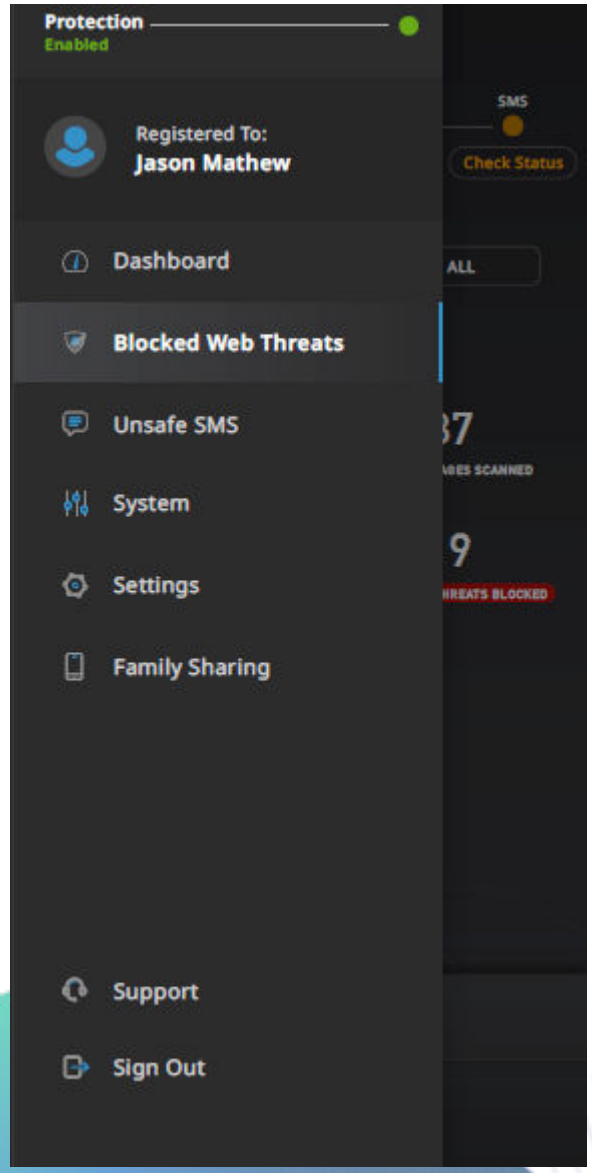
Primary user installing service on their secondary device

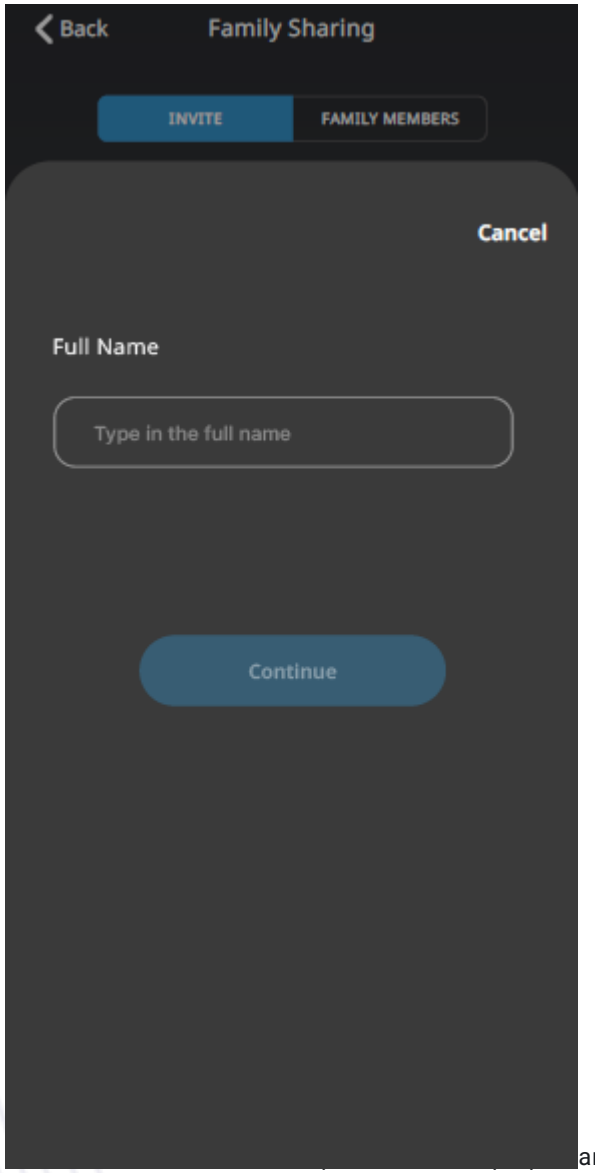


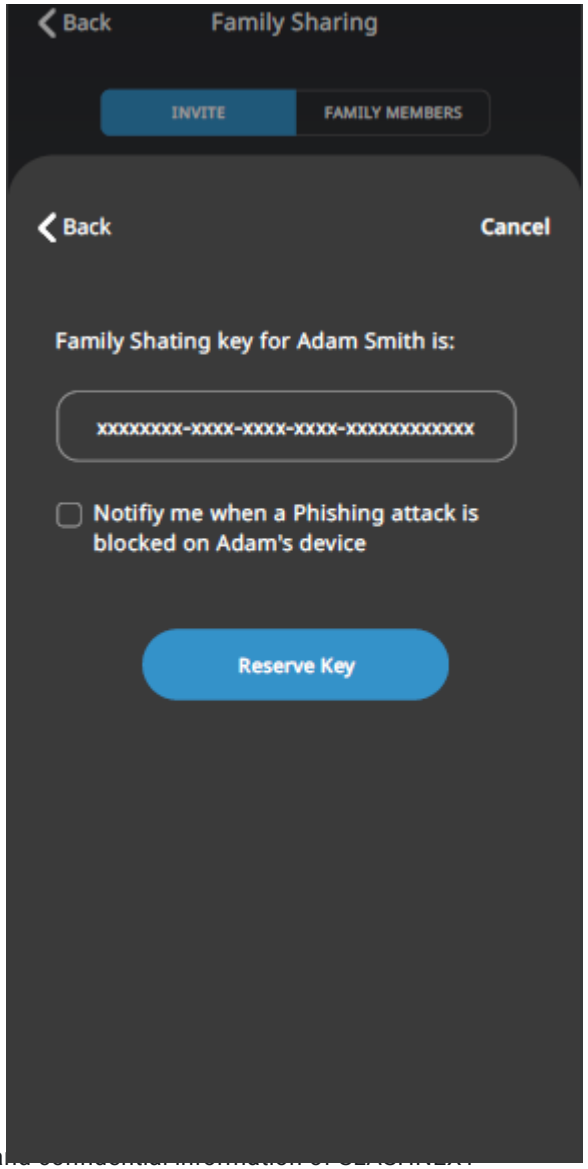


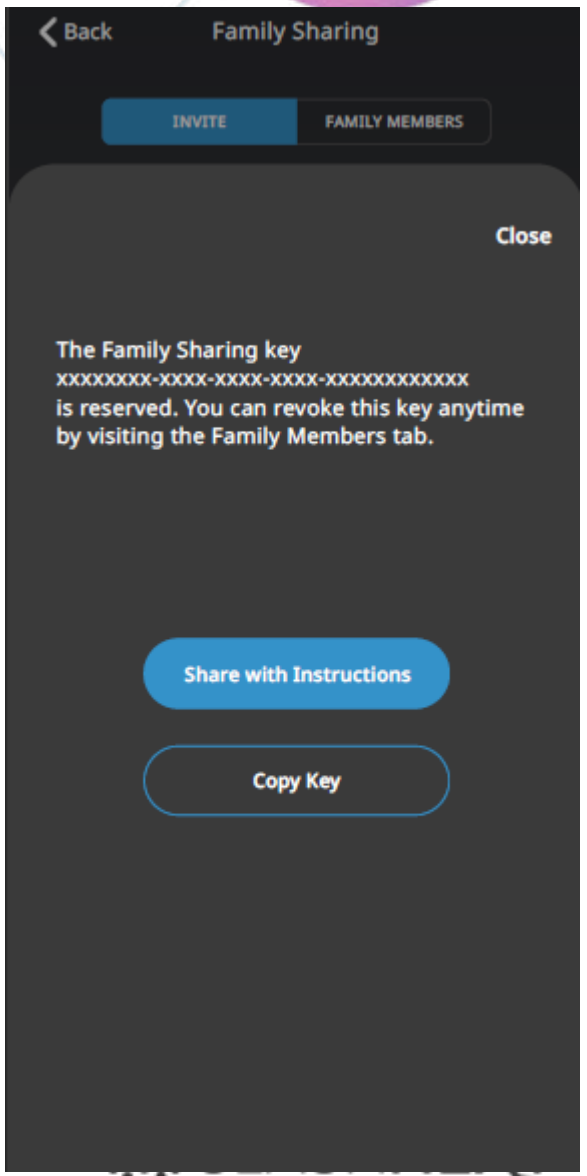
SLASHNEXT

Family Sharing



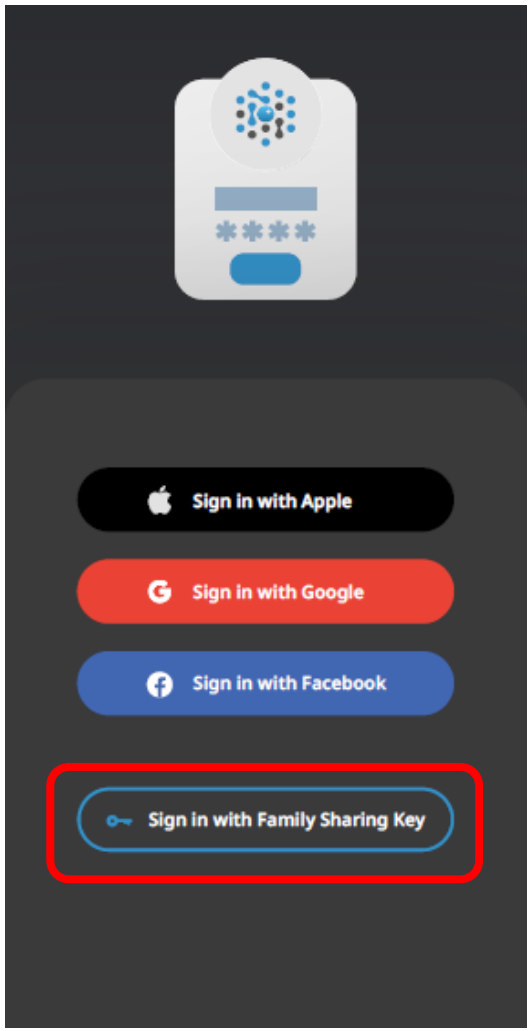


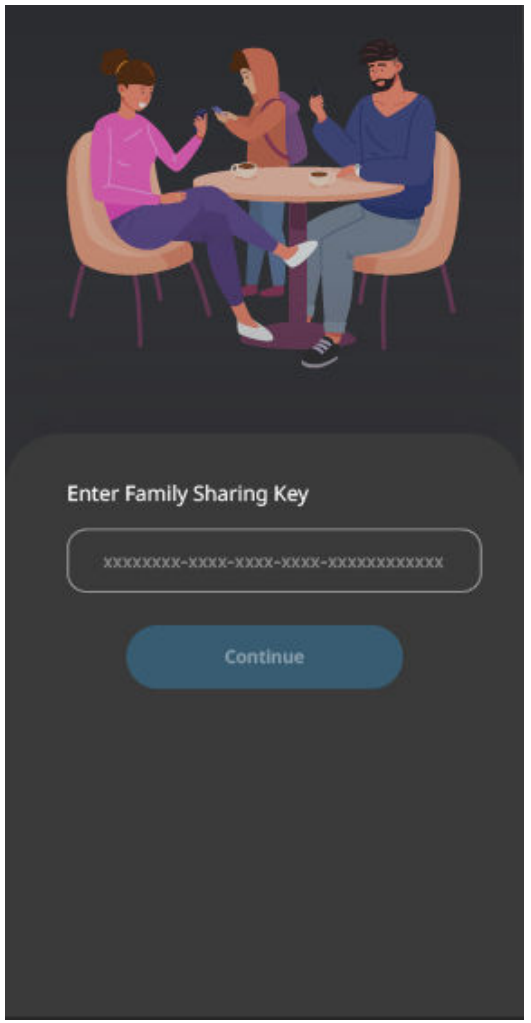


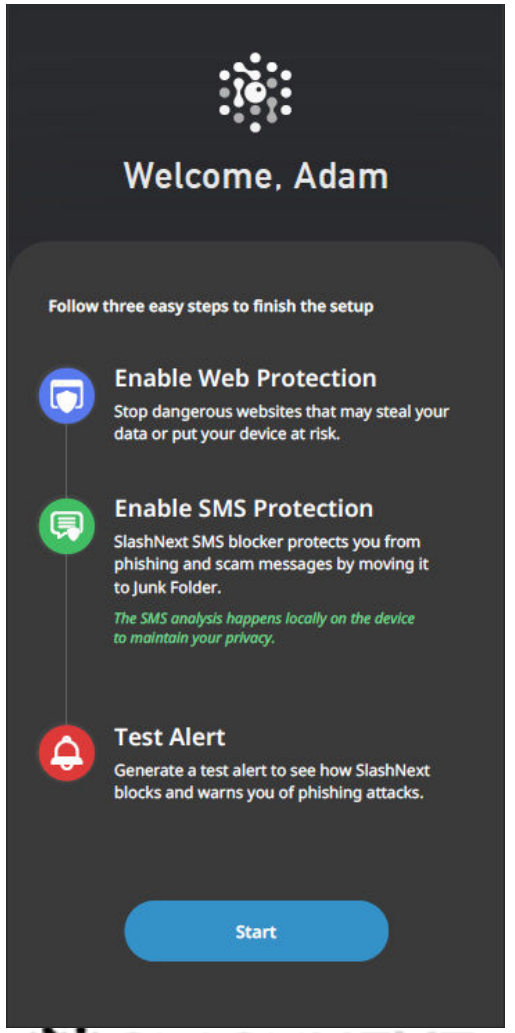


Purchase and Activation

Secondary user activating service on their devices







SLASHNEXT

NOTES

https://www.fortunebusinessinsights.com/parental-control-software-market-104282