

ASHER STAR SECURITY

Security Intruder Plan

November 2025

Contents

| | | |
|----------|---|----------|
| 1 | Introduction | 2 |
| 2 | Phase 1: Sanitize the Device | 2 |
| 2.1 | Goal | 2 |
| 2.2 | Steps and Actions | 3 |
| 3 | Phase 2: Cleaning Facebook (The Core Fix) | 3 |
| 3.1 | Goal | 3 |
| 3.2 | Detailed Procedures | 4 |
| 4 | Phase 3: The Telephony Shield | 5 |
| 4.1 | Goal | 5 |
| 4.2 | Critical Actions | 5 |
| 5 | Phase 4: The Email Perimeter | 6 |
| 5.1 | Goal | 6 |
| 5.2 | Steps | 6 |
| 6 | Phase 5: Locking the Doors (Future Proofing) | 6 |
| 6.1 | Goal | 6 |
| 6.2 | Procedure | 6 |
| 7 | Emergency One-Sheet | 7 |
| 7.1 | Purpose | 7 |

1 Introduction

This document presents a comprehensive and detailed security intruder plan designed by Asher Star Security, intended to counter persistent attacks on personal devices and social media accounts. The objective is to provide a thorough, step-by-step guide for sanitizing the iPhone, securing Facebook and email accounts, and implementing telephony protections to safeguard against intrusions. Each phase includes critical checks and actions to remove possible backdoors and prevent unauthorized access, ensuring long-term protection for the user. Adherence to every step, especially the checks, is imperative even if no immediate threat appears evident.

2 Phase 1: Sanitize the Device

2.1 Goal

Ensure the iPhone itself is not compromised by spyware or unauthorized configurations before entering any new passwords. This foundational step is critical to prevent attackers from intercepting credentials.

2.2 Steps and Actions

| Step | Check | Action |
|--------------------------------|---|--|
| Check for "Spy" Profiles | Navigate to Settings → General → VPN & Device Management. You should see nothing or VPN Not Connected. | If any Configuration Profile or unknown item exists, select it and Delete Profile . |
| Check for "Spy" Keyboards | Go to Settings → General → Keyboard → Keyboards. | Remove all third-party keyboards (e.g., Grammarly or random names) by swiping left and deleting. Keep only English, Vietnamese, and Emoji. |
| Check for Linked Apple Devices | Tap user name/photo at top of Settings; scroll to devices list. | Remove any unknown iPad, Mac, or iPhone by tapping and selecting Remove from Account. |

3 Phase 2: Cleaning Facebook (The Core Fix)

3.1 Goal

Remove any active unauthorized access points, including bots and hidden integrations, that may allow persistent hacker control over Facebook.

3.2 Detailed Procedures

| Check | Description | Action |
|---|---|--|
| Secret Key Check (Business Integrations) | Open Facebook App → Menu → Settings → Apps and Websites and Business Integrations. | Remove all listed items, including old games and business integrations, which often harbor hidden bots like "Night Bot". |
| Rogue Owner Check | Within Facebook Settings, access Accounts Center → Personal Details → Contact Info. | Delete any unfamiliar email addresses or phone numbers immediately to block hacker password resets. |
| Imposter Check | In Accounts Center → Accounts, check linked Instagram or Meta Horizon profiles. | Remove any accounts that are not hers to eliminate unauthorized access. |
| Final Eviction | Go to Password and Security → Where You're Logged In. | Select all device sessions and log out. Then change the Facebook password to a strong, new password. |

4 Phase 3: The Telephony Shield

4.1 Goal

Prevent unauthorized SIM swapping and spoofed phone calls by locking the phone number and filtering unknown calls.

4.2 Critical Actions

| Check | Description | Action |
|---------------------------|---|--|
| Port Freeze (Number Lock) | Call mobile carrier (Dial 611). Request “Port Freeze” or “Number Lock” to prevent SIM swap attacks. | Set a PIN with the carrier and record it securely: _____. |
| Call Forwarding | Navigate to Settings → Phone → Call Forwarding. | Ensure call forwarding is turned off to prevent unauthorized redirection. |
| Silence Unknown Callers | In Settings → Phone, enable Silence Unknown Callers. | This setting sends unknown numbers directly to voicemail, reducing spoofed call risks. |

5 Phase 4: The Email Perimeter

5.1 Goal

Ensure no email filters or rules silently delete or archive security alerts, which might hide intrusion notifications.

5.2 Steps

- Use a computer or official email app (not Apple Mail) to access email settings.
- Locate Filters or Rules within Settings.
- Delete any rule containing keywords like “Facebook,” “Delete,” or “Archive” that may suppress security alerts.

6 Phase 5: Locking the Doors (Future Proofing)

6.1 Goal

Prevent unauthorized changes to important device settings and passwords by enabling Screen Time restrictions.

6.2 Procedure

- Go to Settings → Screen Time.
- Enable Use Screen Time Passcode and set a 4-digit PIN known only to authorized personnel.

- Turn on Content & Privacy Restrictions.
- Under Allow Changes, set Account Changes and Passcode Changes to “Don’t Allow.”

7 Emergency One-Sheet

7.1 Purpose

This page serves as a quick-reference safety guide to protect her from social engineering attacks via phone or messaging.

1. The “Call Back” Rule

If a friend calls asking for money or help sounding unusual: say “I will call you right back,” then hang up and return the call from the contact list to verify identity.

2. The Safe Word

If a supposed relative calls claiming trouble, ask for the predetermined safe word:

Safe Word: _____

If they cannot provide it, hang up immediately; it is likely an automated scam.

3. The “Color Change” Rule

When replying to messages, observe the arrow color:

- **Blue Arrow:** Safe iPhone-to-iPhone communication.
- **Green Arrow:** Standard SMS (Android or unknown numbers).

If a friend who normally shows blue suddenly appears green, stop replying and call them immediately; their number may be compromised.