[redacted]

via eMail

Signal Messenger, LLC
Attn: Privacy
650 Castro Street, Suite 120-223
Mountain View, CA 94041
USA

privacy@signal.org

Partner Marc S. Weidner

Phone
Mobile [redacted]
Telefax
e-Mail [redacted]
Date April 28, 2026
Issued 28.04.2026 07:56:19

Your reference | Your message of

Our reference | Our message of

Proposal Following the Recent Account Takeover Campaign Targeting German Parliamentary Figures

Dear Signal team,

I am writing this as a structured security design proposal, not as a vulnerability report claiming a compromise of Signal's encryption, infrastructure, or application integrity.

The recent public discussion around account takeovers in Germany appears to point to a different class of problem: not a cryptographic break, but a socially engineered account continuity attack. The attacker impersonates "Signal Support", obtains registration credentials or the Signal PIN, takes over the account, may change the associated phone number, prepares the victim for de-registration as if it were expected behavior, and then exploits the victim's confusion during re-registration. The compromised account can subsequently be used to target the victim's contacts from a trusted identity.

That attack path suggests that the vulnerable surface is not message encryption.

The following proposal focuses on privacy-preserving mitigations. It deliberately avoids hardware identifiers, GPS requirements, IMEI or IMSI use, centralized profile-name scanning, message-content analysis, server-side social-graph expansion, or any design that would require Signal to collect more user data. The central premise is simple: critical account actions should be treated as high-risk, transaction-bound identity events, protected by local warnings, explicit intent binding, delayed execution, and optional cryptographic possession proofs.

This proposal responds to Signal's recent public clarification regarding account takeovers reported in Germany, in which Signal correctly distinguished between a compromise of Signal's cryptography or infrastructure and a phishing campaign based on support impersonation, credential disclosure, phone-number change, de-registration confusion, and subsequent abuse of trusted accounts.

1) Threat model

The relevant attack is not merely generic phishing. It is a sequence of identity-confusion steps:

An attacker impersonates Signal Support, Signal Security, Account Recovery, Verification, or similar trusted labels. The victim is persuaded to disclose a registration verification code, Signal PIN, or other account-relevant credential. The attacker registers, migrates, or alters the account state, often including a phone-number change. The victim experiences de-registration and is told that this is expected. The victim then re-registers, believing that they are logging back into the original account, while in fact a new Signal identity may have been created or the previous identity may remain under attacker control. The attacker then weaponizes the trusted account against the victim's contact list.

The important product security problem is therefore account continuity. A user must be able to understand whether they are still controlling the same Signal identity, whether a critical identity transition has occurred, and whether a new registration is restoring the previous identity or creating a new one.

2) Design goals

The proposed mitigations should pursue five goals.

a) Signal should make support impersonation materially harder at the client level without scanning message contents centrally.
b) Signal should distinguish ordinary app state changes from critical identity events. A phone-number change, de-registration, linked-device addition, and account migration should not feel like normal UI flow.
c) Signal should make continuity visible. A user should not have to infer from technical side effects whether they are controlling the same identity.
d) Signal should support a stronger optional protection mode for high-risk users such as journalists, lawyers, political figures, diplomats, activists, civil servants, executives, and security-sensitive organizations.
e) Signal should introduce optional cryptographic possession proof for critical account actions, so that phishing a code or PIN is no longer sufficient in enhanced-risk configurations.

3) Non-goals

The proposal does not require Signal to collect GPS location, IMEI, IMSI, serial numbers, device fingerprints, contact graphs, message content, or profile-name telemetry.

a) It does not propose that Signal become an identity provider.
b) It does not propose central moderation of display names.
c) It does not propose weakening registration privacy.
d) It does not propose making hardware security keys mandatory for all users.
e) It does not assume that every user can manage complex recovery procedures. Stronger controls should be optional, staged, and explicit.

4) Local hard warning for "Signal Support" impersonation

Signal already communicates that Signal Support will not initiate chats or message requests inside Signal. The client should enforce that user's expectation locally.

When an incoming message request from an unknown sender uses a profile display name resembling "*Signal Support*", "*Signal Security*", "*Signal Verification*", "*Account Recovery*", "*Support Team*", "*Security Team*", or comparable variants, the app should display a blocking warning screen. This should be local to the client. No central server-side scanning is necessary.

The warning should not be a small icon. It should interrupt the flow.

Suggested wording:

"*Signal does not provide support through Signal chats or message requests. This message is very likely fraudulent.*"

For the first screen, the reply field should remain disabled. Link previews, QR-code previews, and quick replies should also be suppressed until the user explicitly unlocks the conversation.

The matching should account for obvious evasions: Unicode normalization, homoglyphs, zero-width characters, spacing tricks, and common translated variants of "*support*", "*security*", "*verification*", and "*recovery*". This protection should apply primarily to message requests or unknown senders, where the impersonation risk is highest and legitimate false positives are less costly.

This measure is cheap, local, privacy-preserving, and closely aligned with the reported attack path.

False positives should be handled as friction, not as permanent censorship. The user should retain the ability to proceed after a deliberate override, but the first interaction should be slowed down and stripped of high-risk affordances such as links, QR previews, and quick replies.

This keeps the mechanism compatible with Signal's communication model while making support impersonation materially less effective.

5) Non-imitable official Signal communication

Official Signal security notices should never appear as ordinary chats, message requests, usernames, or profiles.

Signal should maintain a dedicated in-app security notice surface, visually and functionally separate from chats. Any official security communication should appear only through that surface, through previously initiated support correspondence, or through clearly documented official channels.

The client can then state, consistently and repeatedly:

"*Official Signal security notices do not appear as chats or message requests.*"

This matters because phishing is also a language attack. If users are trained that "*support*" can never appear as a chat identity, impersonation loses plausibility.

6) Registration Lock should be presented as account-takeover protection

Registration Lock should be explained more aggressively and more concretely during onboarding and during critical account flows.

A useful formulation would be:

"*Without Registration Lock, someone who obtains your registration verification code may be able to register your number on another device.*"

This warning should appear during onboarding, when requesting a registration code, after de-registration, before phone-number changes, when adding linked devices, and when enabling an enhanced account-protection mode.

For normal users, Registration Lock should remain a strongly recommended control. For enhanced risk modes, it should be mandatory.

Signal should also discourage weak numerical PINs in high-risk configurations and encourage stronger alphanumeric PINs or passphrases.

7) Risk-specific education at the moment of risk

General safety advice is weak because users rarely encounter it at the moment of manipulation. Signal should place short, action-specific warnings directly inside risky flows.

a) When a registration code is shown or sent:
"*This code registers your Signal number on a device. Do not share it. Signal Support will never ask for it.*"

b) When the Signal PIN is requested during registration or re-registration:
"*Entering your Signal PIN here may allow this registration to continue. Signal Support will never ask for your PIN.*"

c) When the app detects de-registration:
"*Your Signal account stopped working on this device because your number may have been registered or changed elsewhere. If you did not initiate this, your account may be at risk.*"

d) When re-registering after de-registration:
"*Re-registering may create a new Signal account. It may not restore your previous Signal identity.*"

The last warning is especially important. Many users interpret "*register again*" as "*log back in*". In an account continuity attack, that ambiguity is exploitable.

8) Treat phone-number changes as high-risk identity transitions

A phone number change should be treated as a critical account action, not as an ordinary profile setting.

In the default mode, Signal should show a clear explanation of the security consequence: the number associated with the Signal identity is changing, and contacts may need to verify the change.

In an enhanced account-protection mode, a phone-number change should trigger a waiting period, for example 24 hours. During that period, the existing primary device should display a persistent cancellation option:

> "*This phone-number change was not initiated by me.*"

If the previous primary device is still active, it should be required to confirm the change. If the previous device is unavailable, a slower recovery path should exist, but it should be visibly different from normal migration.

For institutional or high-risk users, phone-number changes could additionally require a cryptographic possession proof, a hardware security key, or an organization-managed recovery key.

The design principle is straightforward: removing or changing the account's primary routing identifier should be noisy, delayed, and reversible where possible.

9) Make account continuity visible

Signal should introduce an account continuity indicator that distinguishes three states:

a) "Same Signal identity restored."
b) "New Signal identity created. Previous identity not restored."
c) "Previous Signal identity may still be active or controlled elsewhere."

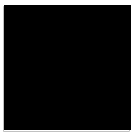
This does not require centralized account history. A device that previously held one Signal identity and now holds another can locally recognize that discontinuity and explain it to the user.

The user-facing distinction matters more than technical precision hidden in a menu. A user should not have to interpret safety-number changes, de-registration events, and missing history to understand whether they are still operating the same identity.

10) Treat de-registration as a security event

De-registration should not be presented as a neutral session interruption.

If an existing device is de-registered because the number was registered elsewhere or because the associated phone number changed, the app should present this as a possible account-security event.



Suggested wording:
"*Your Signal account stopped working on this device because your number may have been registered or changed elsewhere. If this was not you, your account may be at risk.*"

A clear button should be offered:
"*This was not me.*"

That button does not need to promise immediate reversal. It could trigger an incident flow: explain what happened, help the user inspect linked devices, recommend Registration Lock, start a recovery process, temporarily slow further critical account changes where possible, and optionally warn contacts that the account may be compromised.

The essential product change is to break the attacker's narrative. If attackers tell victims that de-registration is expected behavior, Signal should make clear that de-registration can also be an alarm.

11) Contact warnings after critical account changes

When an account changes its phone number, undergoes recent re-registration, or completes a high-risk migration, contacts should receive a clearer security-framed notice.

Suggested wording:
"*This account recently changed its phone number. Verify through another channel before sharing sensitive information.*"

For accounts operating in Enhanced Account Protection Mode, the warning could persist for a limited period. The aim is not to turn every normal phone number change into an emergency. The aim is to reduce the value of a freshly compromised account as a phishing platform against trusted contacts.

Signal already has safety-number and phone-number-change notices. The proposal is to make the security consequence more legible to ordinary users.

Contact warnings should be graduated.

a) A routine phone-number change may justify a neutral notice.
b) A recent phone-number change combined with re-registration, de-registration, or Enhanced Account Protection recovery should justify a stronger security-framed notice.
c) A user reported "T*his was not me*" incident should justify a temporary high-risk warning, subject to careful abuse controls.

The goal is not to create panic around normal account maintenance. The goal is to reduce the immediate trust value of an account that has just undergone a critical identity transition.

12) Prominent account-security status

Security-relevant account state should not be buried. Signal could provide a compact Account Security panel showing:

a) Account identity unchanged since: date.
b) Last phone-number change: date or none.
c) Last linked-device addition: date or none.
d) Registration Lock: enabled or disabled.
e) Linked devices: count and last activity.
f) Last critical account action: date and action.

This panel should be local and privacy-preserving. It should not become a telemetry product. Its purpose is user comprehension: making account continuity visible without forcing users through scattered settings menus.

13) Enhanced Account Protection Mode

Signal should offer an optional Enhanced Account Protection Mode for users with elevated social-engineering risk.

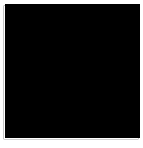
This mode could enable, as a bundle:

a) Mandatory Registration Lock.
b) Stronger PIN or passphrase requirements.
c) Phone-number-change delay.
d) Primary-device confirmation for critical actions.
e) Persistent cancellation window.
f) Clear de-registration alarm.
g) Prominent account continuity indicator.
h) Stronger contact warnings after critical account changes.
i) Restricted linked-device addition.
j) A cryptographic Account Continuity Key for critical account actions.

The mode should be opt-in, because many ordinary users will not tolerate the friction. For high-risk users, that friction is not a nuisance. It is the point.

14) Critical Account Action Confirmation

For critical actions, Signal should use an explicit transaction-bound confirmation ceremony. This should not be a generic "*Are you sure?*" click. Click-through fatigue is one of the attacker's best friends. Before a phone-number change, account migration, identity restoration, or privileged linked-device addition, Signal should show the precise action and its consequence.



Example:
"*You are moving your existing Signal account. After this action, the new device may control your Signal identity.*"

The screen should display, where available and without collecting new data:

a) Old phone number.
b) New phone number.
c) Target device type.
d) Operating system.
e) Time.

The user should then enter a dynamic action-specific sentence.

Examples:

"*I AUTHORIZE CHANGING MY SIGNAL NUMBER TO +41 ...789: 483921*"

"*I AUTHORIZE LINKING A NEW DESKTOP DEVICE: 483921*"

"*I AUTHORIZE RESTORING THIS SIGNAL IDENTITY ON A NEW PHONE: 483921*"

This is not a cryptographic factor. It is intent binding. It prevents accidental approval, QR-code confusion, and reflexive tapping. Against live social engineering, it is not enough. It should therefore be paired with delay, primary-device cancellation, and, in enhanced mode, cryptographic possession proof.

15) Account Continuity Key

The strongest technical measure would be an optional Account Continuity Key.

When Enhanced Account Protection is enabled, the primary device generates an asymmetric key pair. The private key remains locally protected through Android Keystore, iOS Keychain, Secure Enclave, or equivalent platform facilities. Signal's server stores only the public key or an appropriate public-key-derived verifier.

For critical account actions, the server sends a challenge. The primary device signs that challenge. The challenge should bind:

a) Account identifier.
b) Action type.
c) Old phone number, where applicable.
d) New phone number, where applicable.
e) Target device.
f) Timestamp.
g) Server nonce.

The server accepts the critical action only if the signature is valid, or if the user follows a slower recovery path.

This changes the attacker's problem. A phished registration code or PIN is no longer sufficient in enhanced mode. The attacker would need either access to the protected private key or the victim's recovery material.

The design is compatible with Signal's privacy posture because the server does not receive the secret. It only verifies possession.

The Account Continuity Key can coexist with Signal's multi-device model. Linked devices do not need to become equivalent to the primary device by default. Signal could distinguish between ordinary linked devices and continuity-authorized devices.

In the default enhanced model, only the primary device should be able to sign critical account actions. In a higher-assurance institutional model, Signal could optionally support threshold approval, for example one primary device plus one managed recovery key, or one hardware security key plus one administrative recovery mechanism. This should remain optional and should not imply access to message content or message history.

16) Physical access and local user verification

The Account Continuity Key is not meant to protect against an attacker who fully controls an unlocked primary device. It is meant to prevent remote social-engineering attacks in which the attacker obtains phishable credentials such as a registration code or Signal PIN.

In Enhanced Account Protection Mode, signing a critical account action should require local user verification where the platform supports it, for example device passcode, biometric user presence, or OS-backed user-authentication-bound key usage. The confirmation screen should still display the exact action being authorized.

This does not make the mechanism immune to physical compromise. It narrows the attack from remote credential phishing to compromise of the protected primary device or recovery material.

17) Primary device lifecycle and key rotation

For Account Continuity Key purposes, the "*primary device*" should be the device that generated and registered the current continuity key, unless the user explicitly transfers that role.

A primary-device transfer should happen in one of two ways.

The preferred path is signed handover: the current primary device authorizes a new primary device by signing an action-bound challenge that identifies the target device, action type, timestamp, and server nonce.

The fallback path is slow recovery: if the primary device is lost, destroyed, stolen, or unavailable, the user may rotate the Account Continuity Key through an explicitly slower recovery process. This process should require Registration Lock, a recovery artifact or high-entropy recovery key where enabled, a waiting period, and clear warnings on any still-active linked devices.

Key rotation should revoke the previous continuity key and register a new one. During the recovery window, critical account actions such as phone-number changes, linked-device additions, and identity migration should remain delayed or restricted.

18) Recovery file and QR present mode

A recovery file may be useful, but it must not be a bare hash or bearer token.

If possession of a file is sufficient, then whoever copies the file owns the recovery path. A safer design would use an encrypted recovery artifact containing:

a) Encrypted private recovery key or migration secret.
b) Key version.
c) Creation date.
d) KDF parameters, for example Argon2id.
e) Minimal account continuity metadata.
f) Optional Shamir splitting for institutional users.

The recovery file should be protected by a strong passphrase or a high-entropy recovery key.
For institutional use, recovery material could be stored in MDM, HSM, smartcard infrastructure, hardware security keys, or managed secure backup systems.

A QR Present Mode can be useful for local migrations, but it should be short-lived, action-bound, and mutually confirmed on both devices. It should not become a universal recovery bypass that can be captured as a screenshot.

Recovery should restore control, not silently bypass enhanced protections. After successful recovery, Signal should consider placing the account into a temporary protected state. During that period, phone number changes, new linked devices, and further key rotations should remain delayed, visibly logged in the Account Security panel, and optionally announced to existing trusted contacts through security-framed notices.

This prevents the recovery mechanism from becoming a faster attack path than the protected migration flow itself.

19) Implementation phases

The proposal can be implemented in phases.

a) Phase 1: Low-risk, high-value client changes.

   i) Local hard warnings for Signal Support impersonation in message requests.
   ii) Official Signal notices separated from chats.
   iii) Risk-specific registration-code, PIN, de-registration, and re-registration warnings.
   iv) Clear distinction between restored identity and new account.
   v) Prominent Account Security panel.

b) Phase 2: Enhanced account-transition controls.

i) Enhanced Account Protection Mode.
ii) Phone-number-change waiting period.
iii) Primary-device confirmation and cancellation.
iv) "*This was not me*" incident flow.
v) Security-framed contact warnings after critical account changes.
vi) Transaction-bound typed confirmation for critical actions.

c) Phase 3: Cryptographic possession proofs.

i) Account Continuity Key.
ii) Challenge-response signing for critical account actions.
iii) Encrypted recovery artifact.
iv) Institutional policies.
v) Hardware-token support for high-assurance deployments.

20) Expected objections

The first objection is friction. The answer is staging. Ordinary users should receive clearer warnings and better account continuity information. High-risk users should be able to choose stronger controls. Institutions can justify even higher friction.

The second objection is recovery risk. The answer is a slow, explicit recovery path. Security without recovery becomes user hostile. Recovery without friction becomes an attacker's path.

The third objection is privacy. The answer is local decision-making and public-key verification. No GPS, no IMEI, no IMSI, no message scanning, no centralized profile-name surveillance, no expanded social-graph collection.

The fourth objection is warning fatigue. The answer is restraint. Warnings should appear only at critical identity transitions.

The fifth objection is social-engineering resilience. Typed confirmations alone are not enough. They should be treated as intent binding, not as authentication. The stronger layer is cryptographic possession proof.

21) Summary

Signal's encryption is not the weak point in this attack class. The weak point is the account continuity ceremony.

Users can be manipulated into treating de-registration, re-registration, phone-number changes, and account migration as ordinary support-guided procedures. Once that happens, even strong cryptography cannot stop a user from authorizing the wrong transition.

Signal can reduce that risk without compromising its privacy model.

The most important measures are:

a) Make Signal Support impersonation locally and visibly dangerous.
b) Ensure official Signal communication is never presented as chat.
c) Show whether a user has restored the same identity or created a new one.
d) Treat de-registration as a possible account-security event.
e) Treat phone-number changes as high-risk identity transitions.
f) Offer an Enhanced Account Protection Mode.
g) Add transaction-bound confirmations for critical actions.
h) Introduce an optional Account Continuity Key for cryptographic possession proof.
i) Provide safe recovery paths without turning recovery files into bearer tokens.

The core design principle is simple: critical identity transitions should be hard to confuse, hard to rush, hard to impersonate, and, for high-risk users, hard to complete without cryptographic proof of continuity.

Respectfully

[redacted]