FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement

Alert Number: I-032026-PSA | 20 March 2026
Russian Intelligence Services Target Commercial Messaging Application Accounts

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are jointly issuing this public service announcement (PSA) to warn the public about ongoing phishing campaigns by cyber actors associated with the Russian Intelligence Services (RIS) targeting commercial messaging applications (CMAs). RIS actors have compromised individual CMA accounts, but not CMAs' encryption or the applications themselves. The activity targets individuals of high intelligence value, such as current and former U.S. government officials, military personnel, political figures, and journalists.

This global campaign has resulted in unauthorized access to thousands of individual CMA accounts. After compromising an account, malicious actors can view the victims' messages and contact lists, send messages, and conduct additional phishing against other CMA accounts. (**Note:** reporting shows that the threat actors specifically target Signal accounts but can apply similar methods against other CMAs). CMA users who strengthen their personal cybersecurity and defend against social engineering attempts can reduce the risk of account compromise and limit the effectiveness of the threat actors' current tactics, techniques, and procedures.

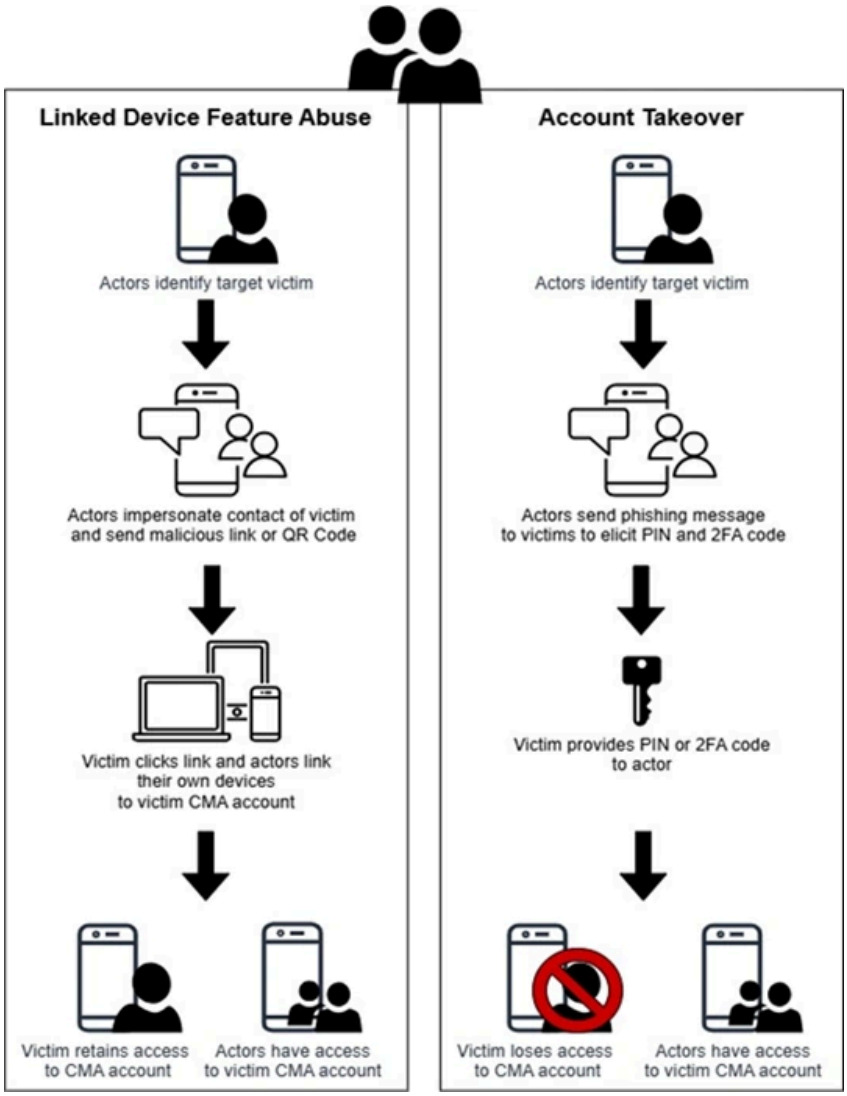

FIGURE 1: TWO SCHEMES

How It Works

RIS cyber actors send phishing messages masquerading as automated CMA support accounts. The actors tailor the messages to deceive targets into taking an action, such as clicking a link or providing verification codes or account PINs (see Figure 2). If the user performs any of the requested actions, they unwittingly provide the actors with unauthorized access to their account either by adding the attacker's device as a linked device or through a full account takeover (see Figure 1). As the campaign evolves, actors may use additional techniques, such as malware to infect the victim.

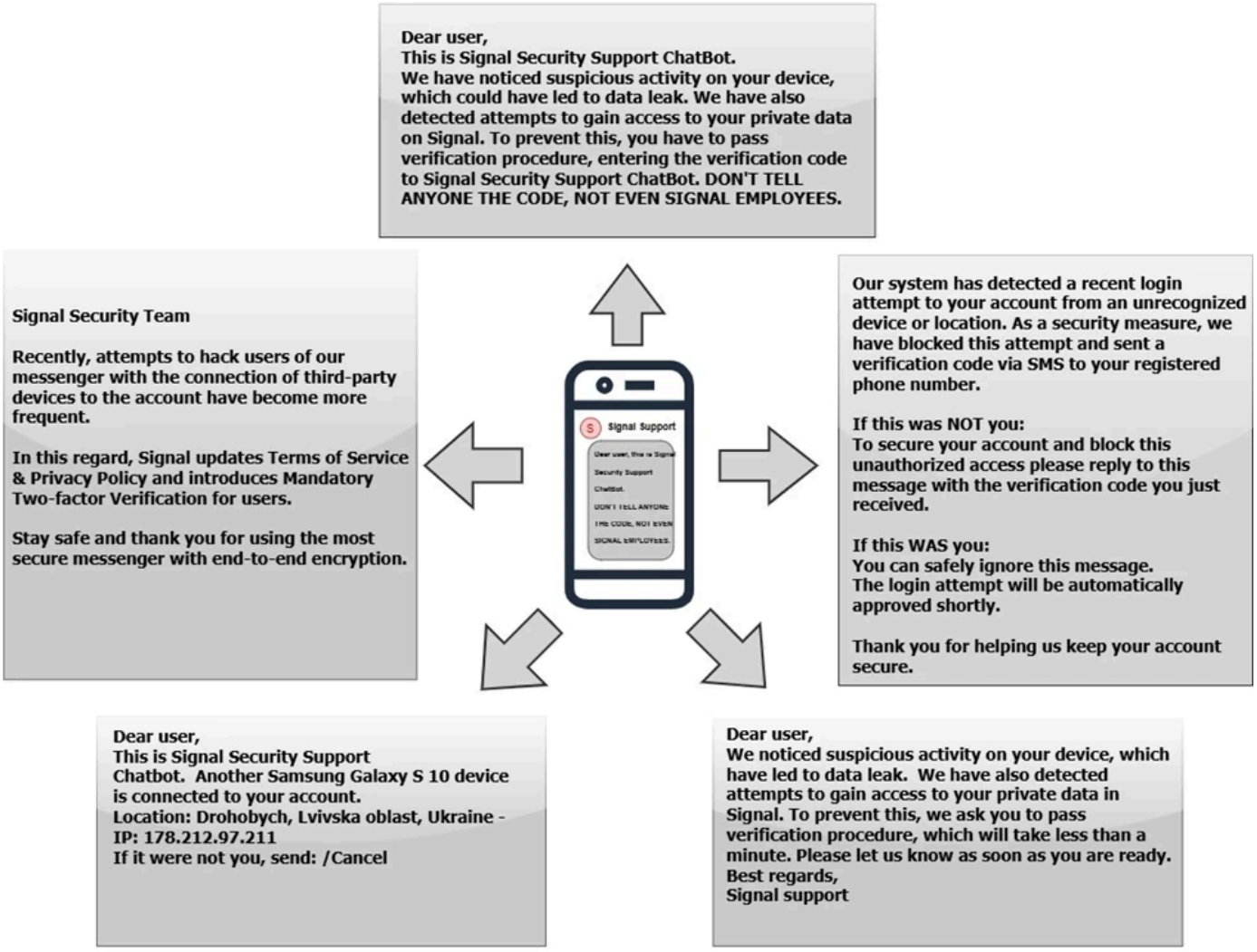

Figure 2: Sample Phishing Messages

Recommendations

Phishing remains one of the most unsophisticated, yet effective means of cyber compromise, often rendering other protections irrelevant including end-to-end encryption. CMA users are urged to be vigilant in identifying potential phishing activity and employing necessary cyber hygiene practices. Users are also reminded to use caution regarding the type of information disseminated and/or discussed on CMAs. While encryption remains effective, phishing allows malicious actors to bypass the encryption entirely by gaining access to user accounts.

The following guidance can be used to identify suspicious messages and help protect yourself from malicious cyber activity:

- **If It Feels Off, Hit Pause:** Suspect a scam? Stop all interaction and do not share codes/PINs/passwords. Never share your PIN or two-factor authentication (2FA) codes for an action you did not initiate.
- **Treat Unknown Messages with Suspicion:** Unexpected messages from unknown contacts (or even "friends" with odd or unusual requests) may be phishing attempts. Block and report these items to

prevent any unauthorized access to your account. If you believe a message may be legitimate, contact the sender through an alternate means of communication to verify before you provide any information.

- **Scrutinize Links Before You Click:** Inspect links and files before clicking or opening. Do NOT click on suspicious links or attachments — it could install malware or enable unauthorized access to your account.
- **Verify Your Group Chats Regularly:** Periodically scan participant lists for duplicates or fakes. If duplicate accounts appear, verify the authenticity of chat participants through another form of secure communication outside of the app.
- **Stay Updated and Locked Down:** Be aware of the security features available within the CMA you use and familiarize yourself with how they work. Enable message expiration features to automatically delete sensitive messages after a set period. For employer-issued devices, verify that applicable records retention policies allow for this setting to be enabled and that doing so is consistent with law.
- **Report Swiftly:** Alert your organization's security team and/or IT department of suspected phishing scams. Additionally, report incidents to the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/ or your local FBI Field Office. For financial or identity fraud, also consider notifying local authorities.
- **Interacting with CMA Support:** Most CMA support services only communicate with users via their official email addresses. Legitimate CMA support services will not request verification codes, especially via direct message within the application itself. CMA support services do not send users links to "verify" or "restore" accounts. Always go directly to the app or official website yourself before interacting with CMA support.

Report It

If you or someone you know has fallen victim to this phishing campaign, file a complaint with IC3. For additional information, see FBI's guidance on Spoofing and Phishing as well as a previous Public Service Announcement about how "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud." Additionally, see CISA's "Phishing Guidance: Stopping the Attack Cycle at Phase One | CISA" and "Mobile Communications Best Practice Guidance."