Fraudsters Targeting AP Staff's Cell and VoIP Phones to Take Over Accounts

To secure your phone systems and protect your accounts, please take a few minutes to follow the steps below.

Across the financial industry, 2023 has started off with a significant number of attacks by fraudsters targeting cellular and VoIP (Voice over Internet Protocol) phones in order to intercept Multi-Factor Authentication (MFA) codes and log in to your bank accounts, emails, and payables systems.

If you log in to your phone online via a website or access your cell phone plan online, there is a risk. Neither of these portals should allow for a Password reset to be done only through email **or** logging in on an unknown device to go unchallenged by MFA.

Most phone providers do not enable critical MFA protection to access their online portals as standard practice and require you to go out of your way and set up Multi-Factor Authentication on those phone login portals.

VoIP Phones

Most VoIP phones are logged into online through a web portal.

Steps to secure these phones

1. Go into your settings, either via your Internet-based system or through the phone itself, and enable multi-factor authentication.
2. Have password reset requests and login confirmations sent directly to a phone in your pocket.
3. Never give an MFA code to any business over the phone. No reputable business will ever ask for them.
4. Never use the same password for your phone login as your computer. If your computer system is taken over, a fraudster will be able to access your phone.

Cell Phones

Fraudsters are trying to obtain a new SIM card for their phones taking over your phone number.

Steps to secure these phones

1. Log in to your online portal for your cell phone provider and ensure MFA is on for your account login is on.
2. Find SIM card security options. This allows you to add another layer of protection even beyond MFA. You can set up a PIN code (usually 4 digits) that is also needed if your SIM card is requested to be transferred to another phone.
3. Create an internal policy to ensure any employee using a personal cell for business use adds these layers of protection to their phones to keep your accounts safe.

Finally, now that your phone is secured, ensure that your email login is secured by MFA. You can find this in settings for many providers or contact your IT department to ensure this is locked down. Many companies use an authenticator app on your phone, as well, which is a highly secure option. This is an added layer even more secure than phone number-based MFA codes. If you have this option, certainly make use of it.

This protection keeps your phones safe, but it also protects your accounts and payments from fraudsters. Any bad actor who has access to your phone can compromise your larger organization, potentially leading to significant losses and risk.

REV US040324PND