Text phishing (smishing) advisory

University leadership has recently been the target of a *text phishing*/*smishing* campaign, where cybercriminals are using mobile text messages to impersonate campus leaders for personal gain. Typically, these types of messages ask someone to open a malicious website and type in sensitive data, such as a password, a PIN, or other personal information, but they can also be as simple as requesting that someone sends money or purchases gift cards.

What is Smishing?

Smishing is a term that combines "SMS" (better known as texting) with phishing. It involves a cybercriminal texting you a request (as described above) while impersonating someone you know.

Phishing is typically a fraudulent email campaign sent out to end users in an attempt to gain sensitive information or compromise login information. Once this information is obtained, threat actors can leverage that login to move within an organization to steal confidential data, plant malware or ransomware, or other malicious acts that may benefit them.

Smishing text messages often appear to be coming from a bank, asking for personal or financial information, or from the local post office to gain other personal information. In CU Denver's recent cases, they appear to be coming from Chancellor Marks or other campus leadership asking for purchases to be made or for personal or financial information to be shared.

Smishing text messages rely on the trust between the person being impersonated and the person receiving the text messages. They will often heighten the target's emotions by creating a sense of urgency and disguise themselves with context that may be believable to override a person's critical thinking skills and spur them into quick action.

How do I identify a smishing text, and what do I do if I see one?

- Slow down, even if a message is urgent. Be skeptical. Ask the question, "does it make sense for this individual to make this request of me?" Generally, answering this question is enough to identify smishing.
- Do not respond. Attackers depend on your curiosity or anxiety over the situation, but you can refuse to engage. Even replying to a prompt like texting "STOP" to unsubscribe can be a trick to identify active phone numbers.
- Check the phone number. Odd-looking phone numbers, such as 4-digit ones, can be sure-fire ways to identify a smishing text. If you have the person saved as a contact, go into your contacts list and verify the phone number is accurate. If it is not, it's likely a smishing text.
- Contact the purported individual directly. If you doubt the validity of the message, contact the person directly (email them or call them on a known number) to verify if the message is real. Do not respond to the text in question!
- Never provide a password or account recovery code via text. Both passwords and text message Multi-Factor Authentication (MFA) recovery codes can be used to take control of your account. Never give this information to anyone, and only use it on official sites.
- Report the event to OIT and let the victim know that this is occurring.

What do I do if I become a victim of smishing?

A victim of smishing is identified as someone who was successfully tricked by the attack – someone that clicked a malicious link, shared a password or identification code, or shared other sensitive information. If you have fallen victim to one of the attacks, you can do the following:

- **Report** the suspected attack to any institutions that could assist.
- **Change** passwords and account PINs where possible.
- **Freeze** credit cards and other financial items to prevent financial loss or ongoing identity fraud.
- **Monitor** finances, credit cards, and various online accounts for strange login locations and other activities.

How do I know if my account is compromised?

- If you can no longer login to your account because the threat actor changed the password or if the account is clearly disabled or locked
- Can't send email to external addresses because Microsoft has blocked it
- Notice missing emails or returned undelivered emails
- Find an unknown forwarding email or deleting email rule in place
- See multiple unknown items appear in the "Sent Items" folder

If your account is compromised, stop all actions, do **not** turn off your computer, and contact the OIT ServiceDesk immediately to report the incident – (303)724-4357 or 4-HELP.

How can we protect ourselves from smishing attacks?

1. **Education.** Any form of phishing, smishing, or social engineering attack can only partially be blocked with technological solutions – solutions that we already have in place. There will always be some that find their way through, and we can only protect ourselves by educating our population.
2. **Spam Blockers**. Spam blockers on email systems are already a best-practice setup in organizations and do block 99% of phishing attacks entering organizations. CU Denver and CU Anschutz does already have these in place. Service providers for phones and text messages are also implementing these for their customers.
3. **Reporting Systems**. These help organizations react when attacks make it through – where emails can be purged from inboxes to protect those who haven't seen them yet, or to send out communications to warn people of particularly sophisticated attack methods. CU Denver and CU Anschutz also has these in place for email systems, with instructions on how to use them on this website.

References

University of Colorado Denver and CU Anschutz Medical Campus (n.d.). *Phishing Attempts*. Office of Information Technology. https://www.ucdenver.edu/offices/office-of-information-technology/it-security/phishing

Kaspersky (n.d.). *What is Smishing and How to Defend Against It?* Resource Center. https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it