Social Media Account Takeover Scams

Author	josh
Date	2023-02-05

Overview

If you are a human with a social media account, scammers want to take it from you. Even if you're like me – not famous, influential or particularly interesting. Scammers use stolen accounts for a variety of purposes, leaving their victims with a frustrating mess to fix. In this article, we'll discuss how social engineers steal your online accounts and how to prevent these sorts of attacks.

Account Takeover

How Scammers Steal Accounts

The fundamental method most scammers use to steal online accounts is *social engineering*. Rather than trying to crack your password (which does sometimes happen) or break Instagram itself, the attacker instead breaks *you*. The goal of the attacker is to trick you into giving them a secret *password reset link.*

A password reset link allows them to change your password to whatever they want and thus take over the account. This "forgot password" feature is useful for you – in the case that, you guessed it, forget your password. However, scammers can initiate a reset by typing your username (public knowledge) into the login form and hitting password reset.

The link is sent to your email or phone number as a way of verifying your identity. While this is going on, the scammers message you with a story such as "I need you to vote for me in a contest. Please screenshot the link I sent to your account" or "I'm locked out of my account and need your help". In any case, they want you to send over this link so they can use it to take your account.

Prevention

There's a simple prevention method for this: *never* give anyone a link that was sent directly to your phone or email. Never copy paste the link, share a screenshot, or use any other method of sending that link to another person, no matter who they say they are. Those links are meant to be *private password reset links* that you, the account holder, use to regain access to an account.

A second way to protect yourself is to use 2 factor authentication (2FA) on any important accounts. 2FA gives a second layer that an attacker must break to take over your account. If an attacker phishes your password reset link, they very likely will also try to trick you into giving a 2FA code. However, this second layer gives you another opportunity to stop, think, and avoid giving the scammer any further information (thus saving your account). These extra layers make it much harder for someone to steal your login.

Keep Your Accounts

There’s a lot of ways we can use the internet to connect with people, knowledge, and tools for good. Unfortunately, scammers love these tools too. The easiest way to steal an account isn’t to break the code directly, but rather to trick you (a silly human) into giving up access to your account instead. Protect yourself by educating yourself on social engineering tactics. Never give anyone a password reset link or 2FA codes – that information is for you only. Stay mindful, stay secure!