INSIGHTS
Cyber made simple.

one brightly cyber

NO NEED TO BREAK IN IF YOU HAVE THE KEY

BY JAY BORDEN

If you watch police procedurals you have probably heard a crime scene investigator say something like “No sign of forced entry. The victim must have known their attacker.” Meaning the attacker was let in by the victim.

In cybercrime there is another possibility, the cybercriminal has your credentials and simply logs in as you. No need to hack into your account. No need to break the security on your computer, tablet, or phone. It’s like leaving a spare key under your door mat. Anyone who knows it’s there, or anyone who chooses to look there can simply use it and walk into your home. No need to pick a lock or break a window.

These actions won’t attract attention from neighbors or in the case of cyber attackers, won’t create an alert or be blocked by protective software like anti-malware, firewalls, access control lists, etc. None of the protections will help if they have your credentials.

How do they get your credentials? They use social engineering to convince your company help desk that they are you and need their password reset. No need to hack your device or buy your credentials on the Dark Web. The Help Desk resets the credentials. Once the cybercriminals do this, the account belongs to them along with all the other access you have. You no longer have access to your account. You may even have difficulty convincing the help desk that you are the legitimate owner of the account and to reset the credentials again.

If you use Multifactor Authentication, MFA, the attackers can get around that again by socially engineering the Help Desk. Attackers have convinced the help desk that they are out of town and using a personal computer and need the new access credentials or change password link sent to their personal email.

onebrightlycyber.com
(888) 773-1920
A global leader in cyber service, technology, insurance and innovation.

NO NEED TO BREAK IN IF YOU HAVE THE KEY

CONTINUED

Sadly, social engineering of the Help Desk works. These types of attacks are also known as malware free attacks because no malware is needed to break in. The percentage of malware free cyberattacks reached 75% in 2023. And is expected to continue to grow.

A recent case where the attackers used social engineering of the help desk gave them six hours of access before it was discovered. By that time the attackers had done their damage installing ransomware and encrypting much if not all the data on the servers. The attackers were so brazen that they even used Microsoft Teams, an application used by the company for inter-team communications, to deliver the notice of ransomware with the amount to be paid to regain access to their information.

Social engineering of help desks has also been effective at mobile communication providers. Attackers convince the mobile provider to reset their password and even to send the 2FA code to them at a new phone claiming they lost the old one. The success rate of this type of attack has been high. Once executed, the attacker has control of the mobile phone account with access to all contacts, calendars, apps, passwords, social media accounts, really anything the legitimate owner does.

The real owner of the account often has a very difficult time convincing their provider that they are the real owner of the account and to reset it again to restore their access. The attackers are more successful than the real owners at convincing the mobile provider that they own the account. It's not uncommon for the real owner to lose all access to their account and need to create a new account with a new mobile number.

So, what can be done?
Educate users to use complex passwords and set security questions.

Consider using passkeys instead of passwords. Passkeys can be more secure as they link to the device. Even if an attacker gets the password and attempts to log in from a different device it will fail.

CYBERTHREATS IN RETAIL

CONTINUED

Equally important, be sure to educate the help desk about social engineering to reduce the chances of that type of attack succeeding. Create policies prohibiting sending credentials to accounts, emails, phones and numbers not registered to the original account owner. No matter how convincing the caller may be.

Be sure the help desk and IT security team work together to scan for suspicious activity and any anomalies. If an unusual request comes in, the help desk should be very wary of granting it.

This is true for emails and other log in information as well as mobile accounts.

Social engineering is successful because help desk personnel are trained to be helpful and are probably helpful by nature. But that is exactly what social engineering exploits.

Remember, as cyber protections get better, attackers get more creative. That doesn't mean they abandon the old attack methods. Anything that works will be used. Don't forget the old ones but always expect something new.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.