

How to Make the IT Help Desk Secure

CHALLENGE: IDENTITY THEFT THROUGH SOCIAL ENGINEERING

In the world of IT, identity theft is a growing concern. Criminals are targeting IT help desks, posing as genuine employees, and manipulating even well-trained support staff into issuing new passwords for intended victims. This stolen password can be a crucial component in various IT attacks, including ransomware assaults.

References show data breaches linked to passwords issued by help desks at major organizations, such as [MGM Casino/Hotels](#), [Caesars Hotels](#), [OKTA](#), [Twitter \(now X\)](#), [Mailchimp](#), [Jumpcloud](#), [CISCO](#), [Lastpass](#), [Twilio](#), [Robinhood](#), and [Reddit](#), and even government agencies like the CIA and FBI falling victim to English teenagers

TRADITIONAL MITIGATION FALLS SHORT

Conventional mitigation strategies involve awareness training, **Multi-Factor Authentication (MFA)** for log-ins, verification procedures, and well-intentioned measures. However, these measures often prove inadequate against skilled social engineers who manipulate emotions to gain the support they need.

The challenge has been compounded by the advent of AI technology, enabling hackers to train computers to emulate a person's voice based on a mere 30-second recording. Users working from home accentuates the issue as we no longer can use internal phone numbers as proof.

THE ULTIMATE SOLUTION: SECURE IT-WORKFLOW

The only foolproof method to safeguard against social engineers stealing passwords from help desks is to [establish a secure IT workflow](#). This workflow, tailored to the user's security profile, can determine precisely how to verify the caller's identity, using dynamic and contextual data that makes it nearly impossible for a hacker to succeed. Remove the supporters' privileged rights to reset passwords.

SOLUTION: FASTPASS

[FastPass offers an innovative solution as a cloud or on-premises offering](#). It has received certification from leading IT Service Management (ITSM) vendors and can seamlessly integrate with almost all ITSM solutions. The [verification process](#) can be customized for different user groups, aligning with your organization's security policies. Additionally, it can incorporate data about the user's device usage, along with the use of Multi-Factor Authentication (MFA).

SUPPLEMENT: ADVANCED SELF-SERVICE FOR PASSWORD RESETS

FastPass goes a step further by providing an [advanced self-service option for password resets](#). This not only reduces the workload on the service desk but also allows more time for a thorough verification process for users seeking personalized assistance. Employees benefit from faster service with no waiting in queues, resulting in enhanced user satisfaction.

In the realm of IT security, safeguarding against identity theft is of paramount importance, and FastPass offers a robust, flexible solution to ensure your organization's defense against social engineering attacks.

CONTACT US:

UK : + 0333 3200513
Europe : + 45 4810 0410

 info@fastpasscorp.com
 www.fastpasscorp.com