The Register®

{* SECURITY *}

Microsoft warns against SMS, voice calls for multi-factor authentication: Try something that can't be SIM swapped

Sending codes over the insecure public telephone network isn't the way to go

Thomas Claburn in San Francisco Wed 11 Nov 2020 // 21:19 UTC SHARE

Microsoft on Tuesday advised internet users to embrace multi-factor authentication (MFA)... except where public switched telephone networks are involved.

Multi-factor authentication, for those who haven't been paying attention, involves adding one or more additional access requirements to password-based authentication. So an online bank, for example, might send a text message to the mobile phone number associated with a given account to make it more likely that the person entering the account password is authorized to access the account.

The technique isn't foolproof though it offers additional defense against attackers who gain access to, or guess through various techniques, the password for a victim's online account. MFA can also be used in conjunction with a password manager: think of multi-factor authentication as an additional layer of protection.

In a blog post, Alex Weinert, director of identity security at Microsoft, says people should definitely use MFA. He claims that accounts using any type of MFA get compromised at a rate that's less than 0.1 per cent of the general population.

At the same time, he argues people should avoid relying on SMS messages or voice calls to handle one-time passcodes (OTPs) because phone-based protocols are fundamentally insecure.

"These mechanisms are based on public switched telephone networks (PSTN), and I believe they're the least secure of the MFA methods available today," said Weinert. "That gap will only widen as MFA adoption increases attackers' interest in breaking these methods and purpose-built authenticators extend their security and usability advantages."

Hacking techniques like SIM swapping – where a miscreant calls a mobile carrier posing as a customer to request the customer's number be ported to a different SIM card in the attacker's possession – and more sophisticated network attacks like SS7 interception have demonstrated the security shortcomings of public phone networks and the companies running them.

Computer scientists from Princeton University examined SIM swapping in a research study [PDF] earlier this year and their results support Weinert's claims. They tested AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless and found "all 5 carriers used insecure authentication challenges that could easily be subverted by attackers."

They also looked at 140 online services that used phone-based authentication to see whether they resisted SIM swapping attacks. And they found 17 had authentication policies that allowed an attacker to hijack an account with a SIM swap.

In September, security firm Check Point Research published a report describing various espionage campaigns, including the discovery of malware that sets up an Android backdoor to steal two-factor authentication codes from SMS messages.

Weinert argues that SMS and voice protocols were not designed with encryption, are easy to attack using social engineering, rely on unreliable mobile carriers, and are subject to shifting regulation.

His answer: Microsoft Authenticator, a mobile app for Android and iOS that allows users to log in using a fingerprint, face recognition, or a PIN in lieu of a password and with an OTP for accounts that support that standard.

"The Authenticator uses encrypted communication, allowing bi-directional communication on authentication status, and we’re currently working on adding even more context and control to the app to help users keep themselves safe," said Weinert. "In just the last year, we’ve added app lock, hiding notifications from the lock screen, sign-in history in the app, and more – and this list will have grown by the time you plan your deployment, and keep growing while SMS and voice keep sitting still."

For those made uneasy by more Microsoft gatekeeping, there are alternatives, like Twilio's Authy, Cisco's Duo Mobile, Google Authenticator, and password managers like 1Password and LastPass. Any of these would be an improvement over SMS and voice. ®

MORE Microsoft Security

Corrections Send us news

69 Comments

// **KEEP READING**

Microsoft makes cloudy Linux licensing less labyrinthine

Tickles the Azure Hybrid Benefit so that RHEL and SUSE users get the same deal as Windows buyers