CLOUDFLARE

CASE STUDY

The (hard) key to stop phishing

How Cloudflare stopped a targeted attack and you can too

The account takeover problem

Hackers don't break in, they log in

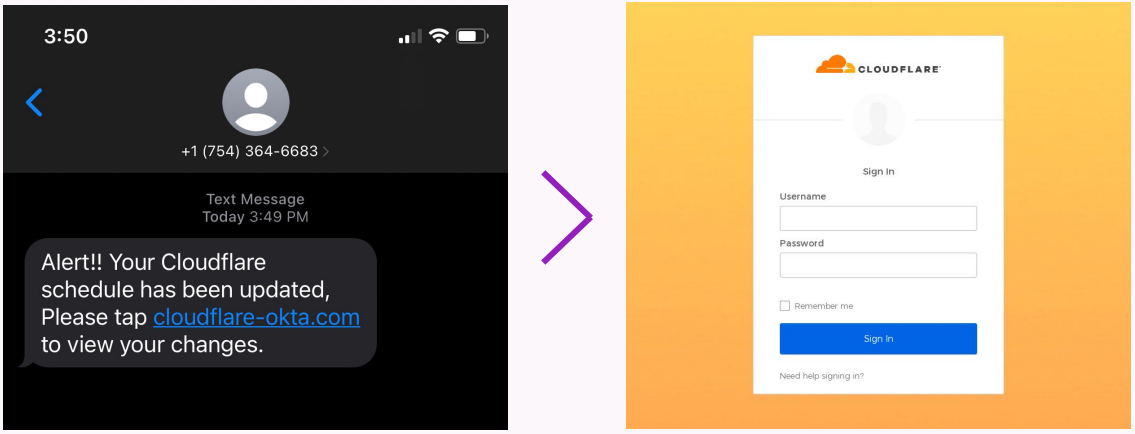
More organizations today are finding themselves victims of attempted account takeover attacks, in which threat actors send socially-engineered SMS text messages to company employees with the aim to phish and harvest identity provider (IdP) login credentials. By gaining unauthorized access, the threat actors can move laterally to steal not only employee information but that of downstream customers as well.

Cloudflare has not experienced any successful account takeovers since we rolled out security keys replacing time-based one-time password (OTP) applications. In July 2022, Cloudflare once again thwarted a sophisticated attack largely thanks to FIDO2-compliant YubiKeys required for multifactor authentication (MFA).

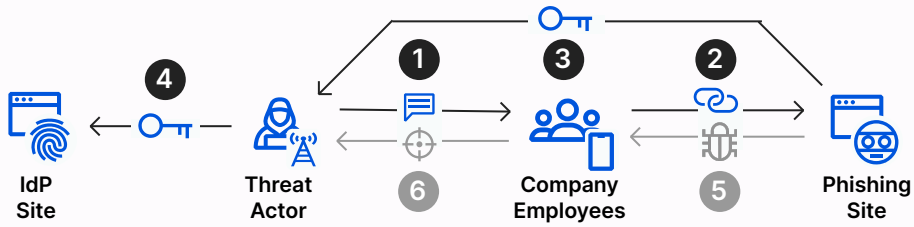
> **"On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare Okta login page... While the attacker attempted to log in to our systems with compromised credentials,**
>
> **they could not get past the hard key requirement."** [1]
>
> CLOUDFLARE

What Cloudflare employees saw

76 employees received legitimate looking text messages within one minute of the attack launch, containing both the words "cloudflare" and "okta." If clicked, the link brought employees to an identical replica of an Okta login page for credential harvesting.



July 20, 2022 attack details



Phase	#	What happened	Technical details	Cloudflare's response
Targeted texts	**1a**	Threat actor sent legitimate-looking malicious SMS	100+ messages sent from four T-Mobile-issued SIM cards	9 min after attack, SIRT sent an internal warning to all employees across chat & email
	1b	Company employees and family members received SMS on personal and work phone #s	76+ employees received in <1 min	1 min after attack, SIRT team was informed; no evidence of compromise via directory provider logs
	2a	Message included a legitimate-looking newly registered domain (cloudflare-okta.com)	Domain registered via "Porkbun" <40 min before the phishing campaign began to avoid automated detection	3 min after attack, SIRT added domain to SWG to block access. Later, isolated access to all newly registered domains and seized control of domain.
	2b	Clicking link opened a legitimate-looking phishing site (Cloudflare Okta login page)	Site had a Nuxt.js frontend, a Django backend, and was hosted on DigitalOcean	37 min after attack, DigitalOcean shutdown the attacker's server via our collaboration
Real-time phishing	**3a**	Victim's entered credentials were immediately relayed to the threat actor	Telegram messaging service provided real-time relay	1-37 min after attack, SIRT killed active sessions via ZTNA, and 48 min after attack, also SIRT reset credentials & initiated scans for the identities & devices with unverified 2FA per our activity logs
	4a	Threat actor enters credentials received into actual identity provider (IdP) login site; sending TOTP codes to victims via SMS or mobile app	IdP site was accessed by VPN software IPs via a dedicated server provider	Intel from server indicated actor was targeting other orgs, including Twilio, and SIRT shared intel SIRT blocked IPs used by threat actor from accessing any Cloudflare service
	3b	Victim enters TOTP code on the phishing site, and it too would be relayed to the threat actor	3 employees reached this step, but did not go further as hard keys don't use TOTP	n/a
	4b	Threat actor enters code in IdP site before it expires	Defeats most 2FA implementations	n/a
Remote access	**5**	Phishing site initiated download of a phishing payload (may have been due to a misconfigured kit)	Included AnyDesk remote access software	n/a
	6	Once software installs, threat actor controls victims' machine remotely	n/a	Endpoint security used by Cloudflare would have stopped the installation

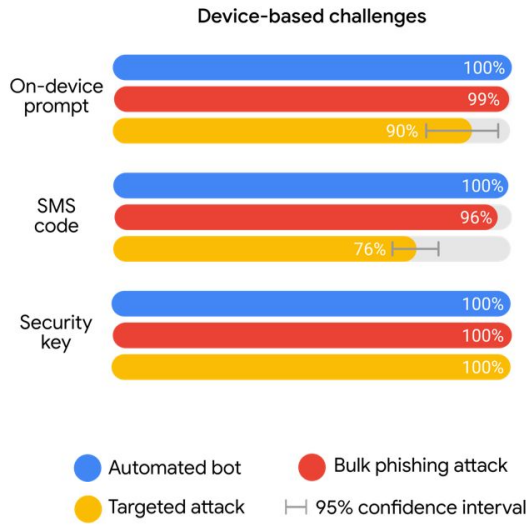
Other security learnings from the attack

- Cloudforce One also had identified the phishing domain and blocked it but not before some employees had clicked on the links, so our engineering will speed up this identification process.
- Cloudflare Gateway already offered the newly seen domain security risk category to customers but Cloudflare Security had not implemented ourselves.

Adopt phishing-resistant MFA

Any form of MFA is better than none given the prevalence of stolen credentials, but not all MFA provides the same level of security. A spectrum of less secure MFA methods like SMS or time-based OTP (or especially knowledge questions) should be replaced with more proven methods like FIDO2-compliant MFA implementations.

Google research[2] has also shown that hardware security keys are among the most secure authentication methods in existence today. The chart to the right shows account takeover prevention rates by challenge type.



Get rid of TOTP apps

Threat actors can still take advantage of TOTP through on-path, man-in-the-middle attacks as seen by the attempted attack on Cloudflare. Other OTP methods like SMS are similarly vulnerable through techniques like SIM swapping.

Adopt FIDO2-compliant keys

FIDO2 achieves verification and strong authentication with public key cryptography. Identification can be embedded into physical media devices like security keys or even built-in device options like Windows Hello.

Ensure compatibility

Not every Internet, SaaS, or self-hosted application will natively support FIDO2 authentication; IAM and ZTNA services can help extend its reach. You may also need a tangential strategy for WebAuthn in the mobile context.

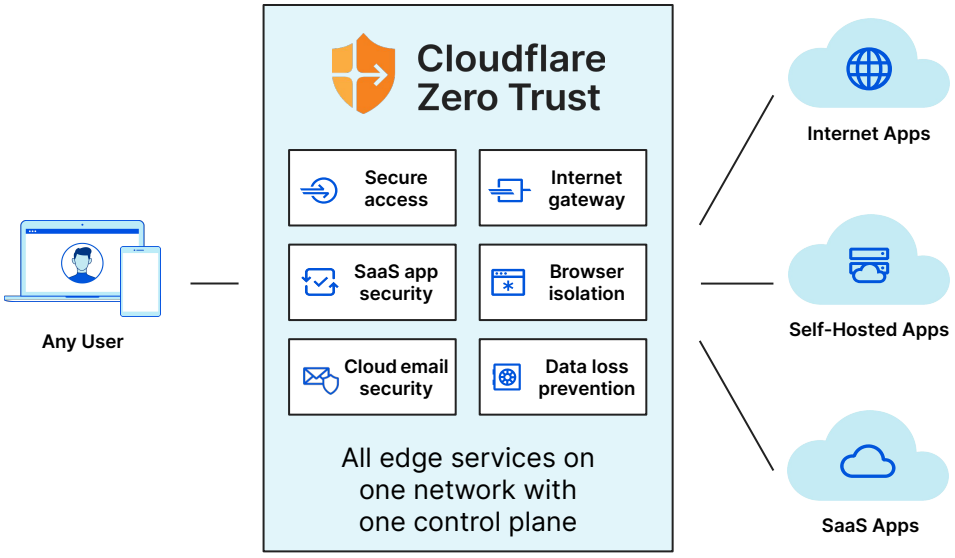
Other strong authentication recommendations:

- Selectively enforce strong authentication as needed. ZTNA can also help overcome this shortcoming with some IAM providers and help require FIDO2 authentication for higher risk apps.
- FIDO2-compliant keys are not automatically compatible with all apps. Use a Zero Trust Network Access (ZTNA) service to help roll out strong authentication to all your resources.

Adopt Zero Trust via one platform

At Cloudflare, we use our own Zero Trust platform to protect all of our users and resources. Several of the component services played a role to help mitigate the targeted attack.

While ZTNA spread the reach of our YubiKeys to ensure strong authentication on every app, Zero Trust services also helped our security team block the phishing domain quickly, kill compromised sessions, audit activity logs, and tighten additional preventive measures for the future.



How ZT services can help

Block phishing domain w/SWG

Kill active, compromised sessions w/ZTNA

Search ZTNA/SWG logs for impacted users
see who clicked what to take better action

Run suspicious sites & email links thru RBI
including newly seen or new domains

Block sites before campaigns launch w/CES
scan web for phishing sites

First best practice from Cloudflare IT

- **Enable easier, faster operations** by consolidating ZTNA with SWG into one platform.
- **Prevent further attack spread** and next steps like ransomware.

Second best practice from Cloudflare IT

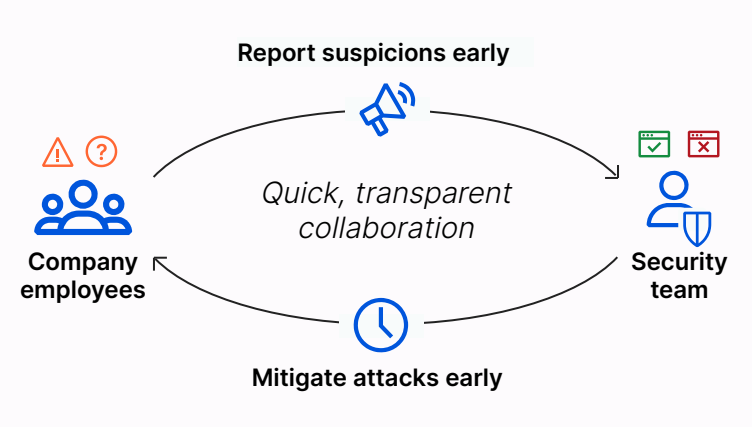
- **Improve security posture** by expanding platform with RBI, CES, CASB and DLP.

Establish a paranoid, blame-free culture

Cloudflare's security mindset before this attack

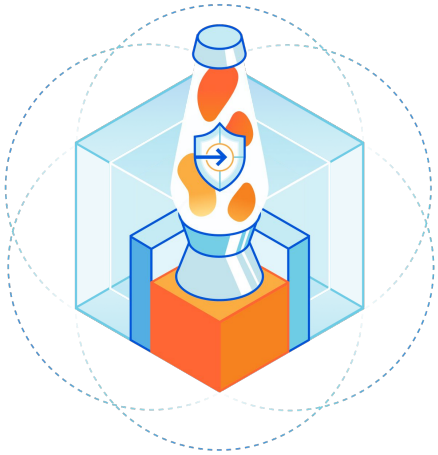
- Security team is also a product team
- Customer data is more precious than ours
- Security is part of everyone's job

Cloudflare operates its own internal 24×7 Security Incident Response Team (SIRT) and encourages all employees to report suspicious activity early and often. We use our own security products every day, helping us continually improve the direction of our products through actionable insights from real cyberattack response and mitigation.



Culture starts with leadership

Cloudflare encourages an open, transparent "see something, say something" approach to collaborating with SIRT, creating a strong internal first line of defense. More than 90% of employee reports to SIRT are benign, which leadership reinforces is expected and okay. Genuine mistakes are also okay and should be reported as soon as possible, because minutes matter during real attacks.



1. Cloudflare blog post, August 9, 2022, "The mechanics of a sophisticated phishing scam and how we stopped it" blog.cloudflare.com/2022-07-sms-phishing-attacks/