Reddit Feb 2023 Social Engineering Attack and Data Breach

Incident Name	Reddit Feb 2023 Social Engineering Attack and Data Breach
Date of Incident	February 5th, 2023
Summary	Reddit, a popular news and social media platform, announced recently that on February 5, 2023, the company suffered a data breach. The breach occurred after Reddit employees were targeted with a phishing campaign. As a result of the campaign, one of Reddit's employees entered their credentials and multifactor token into a spoofed Reddit site that was created by the attacker. The attacker was then able to access internal documentation, code, internal dashboards, and business systems. Reddit has stated that no user accounts were breached in this attack and that the attacker did not gain access to production systems. Reddit responded very quickly to the incident and was able to remove the attacker from its systems after being notified of this breach by the employee who fell for the phishing campaign. The company is currently investigating this incident and looking at improving its security posture, including enhanced employee training. Reddit has also reminded users to use a password manager and enable 2FA on their accounts for extra protection. When Reddit announced this breach, the company ran an AMA on its platform for users to ask questions. There are currently no details on who carried out the attack and if the stolen data has been leaked. Back in 2018, Reddit reported a security breach in which an attacker was able to get access to some of the company's systems, user data (emails), and a 2007 database backup containing salted and hashed passwords. It was found that the attacker breached employee accounts on Reddit's cloud infrastructure, which required employees to use an SMS-based second factor of authentication. As a result of this previous incident, Reddit has since encouraged employees to use a token-based 2FA method instead.
Key Social Engineering /OSINT Themes	• Recon - Reddit employee and organizational information harvested. The hacker leveraged exposed employee information to conduct a social engineering attack. • Phishing - The attacker sent a convincing phishing email to certain employees which prompted them to click on a link. Once the user clicked on this link, they were presented with a legitimate looking Reddit site that prompted them for credentials and for their 2FA token. The attacker then used these to gain unauthorized access.
Remediations	• User social engineering awareness training • Identify and block newly registered domains similar to your org's. This way if used in an attack (e.g., user clicking), the request to domain is blocked. • Monitor for expiring domains which could be leveraged for the above. • Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts. • Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party. • Regularly audit employee access to one of least privilege (including offboarding). • Regularly audit 3rd party access to one of least privilege. • Monitor and remove sensitive information disclosure.
Industry	Social Media
Actor	TBC
Motivations	TBC

Related Hacks	Riot Games
Breach Notice/Company Notice	https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/
Other Sources	https://www.bleepingcomputer.com/news/security/hackers-breach-reddit-to-steal-source-code-and-internal-data/ https://www.darkreading.com/risk/reddit-hack-shows-limits-mfa-strengths-security-training https://www.forbes.com/sites/daveywinder/2023/02/10/reddit-confirms-it-was-hacked-recommends-users-set-up-2fa/ https://www.ncsc.gov.uk/guidance/ncsc-advice-reddit-users https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/ https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/