FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement

Alert Number: I-090126-PSA | 01 September 2026
Malicious Cyber Actors Gain Access to Victim Accounts Through Consent Phishing

Since late 2025, malicious cyber actors have been targeting prominent victims, their family members, and personal acquaintances by directly messaging personal accounts with malicious links leveraging a technique known as "OAuth consent phishing."

Threat Landscape

> ***OAuth*** *is a commonly used authorization framework which enables websites and Web applications to request access to a user's account on another application without the user exposing their login credentials to the requesting application.*

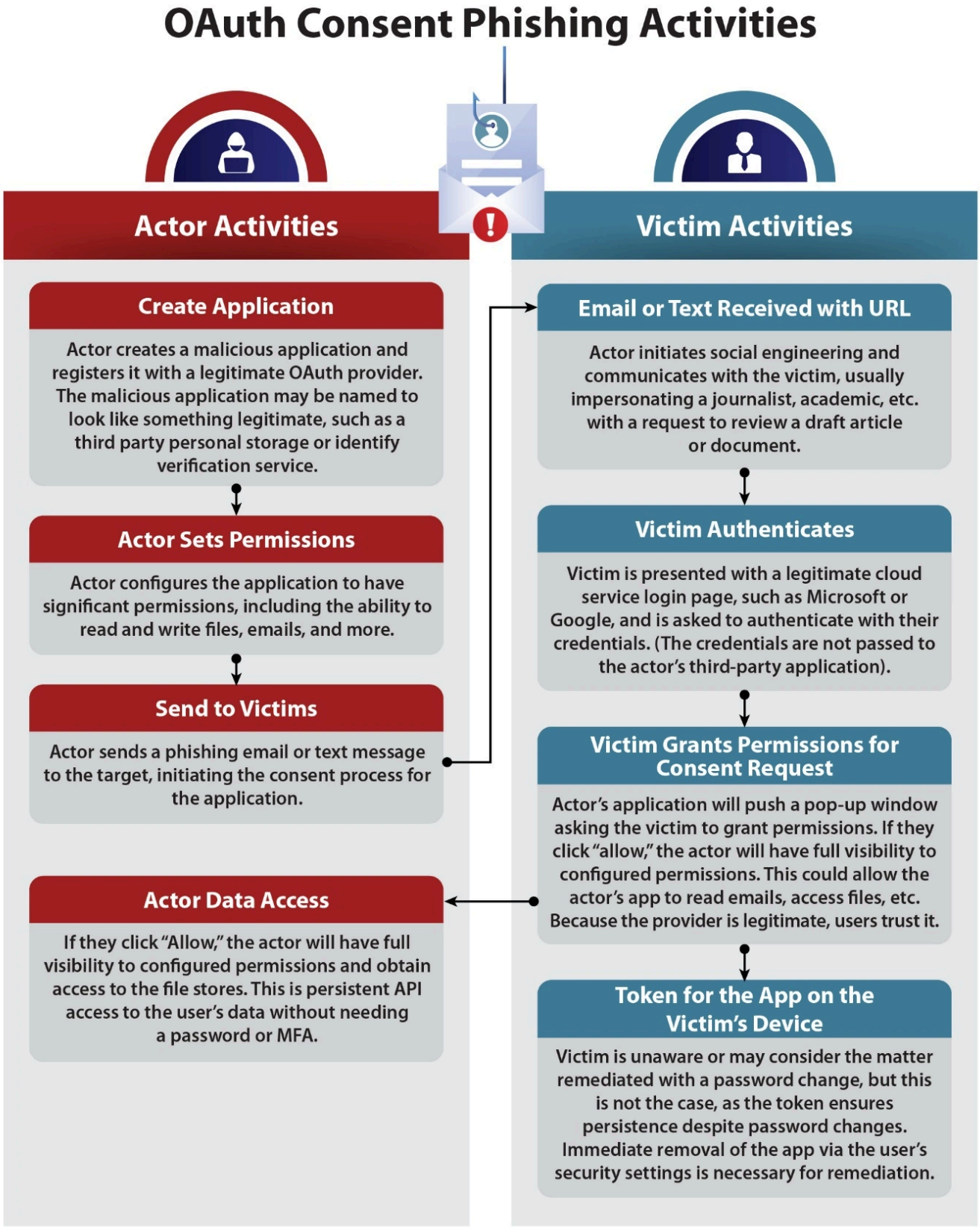
Recently observed activity includes impersonating government officials, media, and other publicly known personalities on a commercial messaging application (CMA) and soliciting the targeted individual to access a malicious link under the guise of a file sharing service through an application under the malicious actor's control. Previous phishing campaigns have also impersonated event coordinators and planners, who sent malicious links to targets under the guise of an invitation to an event and the need to verify the target's identity through a malicious application under the actor's control.

How OAuth Consent Phishing Works

Historically, spear phishing efforts focused on social engineering ruses with links or access to malicious credential harvesting sites or malware deployment to gain access to target accounts or devices. OAuth consent phishing provides actors with persistent access to a target's account because once permission is obtained, it can only be revoked by the victim invalidating the token in their application security settings; not by changing the password.

OAuth consent phishing is a deceptive, sophisticated approach to access user accounts without requiring a password. It typically begins with a phishing email or direct message through a CMA and, when the user clicks the malicious link, they are redirected to a legitimate communication provider permission request screen. If the user approves the request, they unwittingly grant high-level access to a malicious application controlled by the cyber actor. From that moment, the cyber actor can act on behalf of the user, including reading and sending emails, and accessing sensitive data without having access to the user's credentials. By registering malicious applications through legitimate authorization protocols and

using social engineering tactics, cyber actors can bypass both passwords and multi-factor authentication, which makes consent phishing especially dangerous.



Tips to Protect Yourself

Mitigation strategies include increased scrutiny of communications from unfamiliar phone numbers, accounts, or that are not part of a known contact list. Additionally, independently verify the identity of the sender and only grant authorization to trusted applications.

Report It

If you believe you have been the victim of the phishing campaign described above, contact your relevant security officials. The FBI requests victims also report any incident to their local FBI Field Office or the Internet Crime Complaint Center (IC3) at http://www.ic3.gov. Report information elicited and maintain screenshots of messages.