# GitHub is under strong phishing attack, users pay attention to account security

GitHub - the world's largest open source software repository, is now the target of a phishing attack campaign.

GitHub - the world's largest open source software repository, is now the target of a phishing attack campaign specifically designed to collect and steal city credentials. members through fake websites that imitate the GitHub login page.

In addition to hijacking a Github user account, the attacker will also immediately download the entire contents of the victim's private repositories, including but not limited to "properties owned by the account. organizations and other contributors ".

'If attackers successfully steal GitHub user login credentials, they can quickly create a GitHub personal access token or authorize OAuth applications on the account to maintain permissions. Access in case of victims 'password changes,' said GitHub's security incident response team (SIRT) in a warning.


GitHub

## Phishing attacks targeting active GitHub accounts

Through phishing emails, hackers use many different types of 'lures' to trick the target into clicking the attached malicious link. In the event that GitHub users are fooled and click on a link to check their account activity, they will be redirected to a fake GitHub login page, designed to be 99% authentic. If the victim does not recognize and enter the login information as usual, their entire account login information will be saved and sent to the

server controlled by the attacker.

In addition, the fraudulent landing page will also filter the victim's 2FA code in real time if they are using a mobile application with a one-time-based password algorithm (TOTP). This malicious mechanism allows an attacker to easily gain access to a protected account using a two-factor authentication method based on TOTP.

*"However, accounts protected by hardware security keys will be virtually unaffected by this attack,"* SIRT said.

This ongoing fraud campaign targets GitHub users who currently operate for technology companies in various countries, using email addresses obtained from public commitments.

In particular, phishing emails are sent from legitimate domain names, using previously compromised email servers, or with the help of stolen API information from legitimate bulk email service providers. .

In addition, the attackers behind this campaign also use URL shortening services designed to hide the URL of the landing page, and combine a series of URL shortening services to enhance cloaking. . In addition, to make the malicious links attached to emails harder to identify, they also use PHP-based redirects on compromised websites.

## Security recommendations from GitHub

The recommendations made by the SIRT team for Github users are as follows:

1. Reset account password immediately.
2. Reset the two-factor recovery code immediately.
3. Review the personal access token.
4. Take additional steps to better control and secure your account.
5. Consider using hardware security keys and using a password manager integrated with the browser.
6. Be wary of any incoming emails.