



Advanced Phishing is Targeting Your Backups




Oauth phishing

This type of phishing attack targets users of the Oauth protocol that provides authentication services for most SaaS integrations. Oauth phishing emails contain a fake link that redirects the victim to a malicious website that looks identical to the real Oauth website. The victim is then prompted to enter their login credentials, which are then stolen by the attacker.



Spear phishing

Spear phishing is a type of phishing attack that targets a specific individual or organization. The attacker will often conduct extensive background research on the victim to personalize the phishing email and make it seem more believable. For example, an attacker might include the name, title, or company name of the victim in the email.



Personalized SMS messages (smishing)

Smishing is a type of phishing attack that uses text messages instead of email. The attacker will send a text message to the victim that contains a fake link. When the victim clicks on the link, they are taken to a malicious website that looks identical to the real website. The victim is then prompted to enter their login credentials, which are then stolen by the attacker.



Third-party phishing

Third-party phishing is a type of phishing attack that uses a third-party service, such as an email marketing platform or a social media site, to send phishing emails or messages. The attacker will create an account on the third-party platform and use it to send phishing emails or messages to the victim.



Whaling

Whaling is a type of phishing attack that targets high-profile individuals, such as CEOs or CFOs. The attacker will often research the victim to personalize the phishing email and make it seem more believable. For example, the attacker might include the name or company name of the victim in the email.



Vishing

Vishing is a type of phishing attack that uses voice calls instead of email or text messages. The attacker will call the victim and pretend to be from a trusted organization, such as a bank or government agency. The attacker will then try to trick the victim into sharing personal information, such as login credentials or credit card numbers.




Email phishing

Email phishing is the most common type of phishing attack. The attacker will send an email to the victim that contains a fake link. When the victim clicks on the link, they are taken to a malicious website that looks identical to the real website. The victim is then prompted to enter their login credentials, which are then stolen by the attacker.



SEO phishing

SEO phishing is a type of phishing attack that uses search engine optimization (SEO) to rank high in search results for specific keywords. The attacker will create a phishing website and optimize it for certain keywords. When the victim searches for those keywords, the phishing website will appear high in the search results. The victim is then taken to the phishing website where they could be duped to click on malicious links or reveal their login credentials.



Hackers use phishing tactics to steal your credentials and delete backups as the first step in a ransomware attack. Asigra Tigris backup is equipped with deep MFA to prevent unauthorized logins and to ensure your Asigra backup system won't be compromised even when phishing attacks are successful, and attackers penetrate the network.

Ready to learn more?
Email marketing@asigra.com

asigra