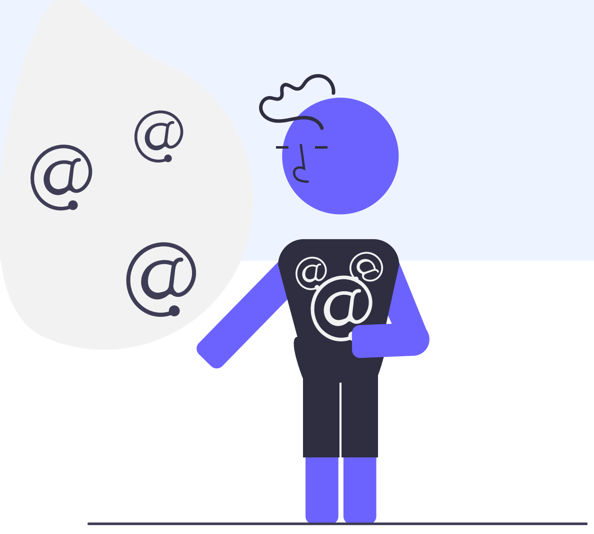
Types of Phishing

Email phishing

Phishing attacks, often delivered via email spam, attempt to trick individuals into giving away sensitive information or login credentials. Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience.

01



Spear phishing

Spear phishing is a targeted phishing attack that uses personalized emails to trick a specific individual or organization into believing they are legitimate. It often utilizes personal information about the target to increase the chances of success.

02

Whaling and CEO fraud

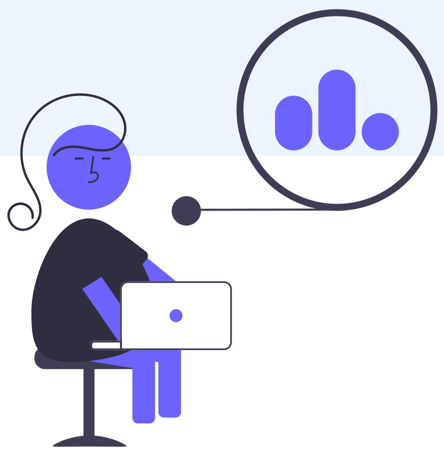
Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals with customized content, often related to a subpoena or customer complaint.

03

Clone phishing

Clone phishing is a type of attack where a legitimate email with an attachment or link is copied and modified to contain malicious content. The modified email is then sent from a fake address made to look like it's from the original sender.

04



Voice phishing

Voice over IP (VoIP) is used in vishing or voice phishing attacks, where attackers make automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts. The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution

05

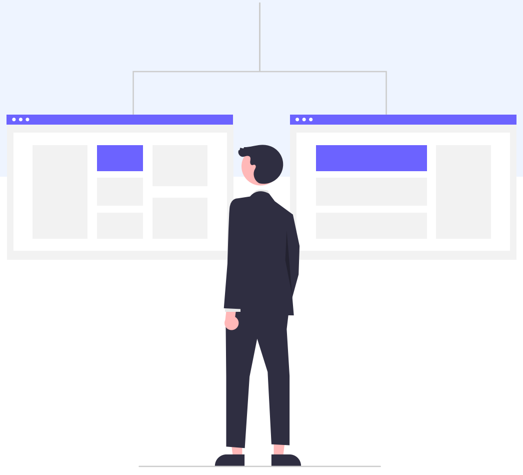
iq.global/phishing

Types of Phishing

SMS phishing

SMS phishing or smishing is a type of phishing attack that uses text messages from a cell phone or smartphone to deliver a bait message. The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.

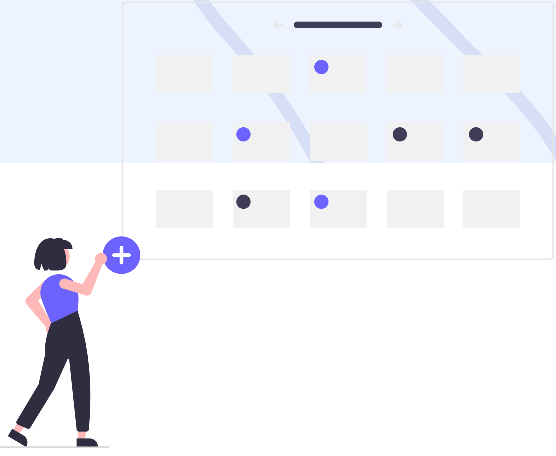
06



Page hijacking

Page hijacking involves redirecting users to malicious websites or exploit kits through the compromise of legitimate web pages, often using cross site scripting. Hackers may insert exploit kits such as MPack into compromised websites to exploit legitimate users visiting the server.

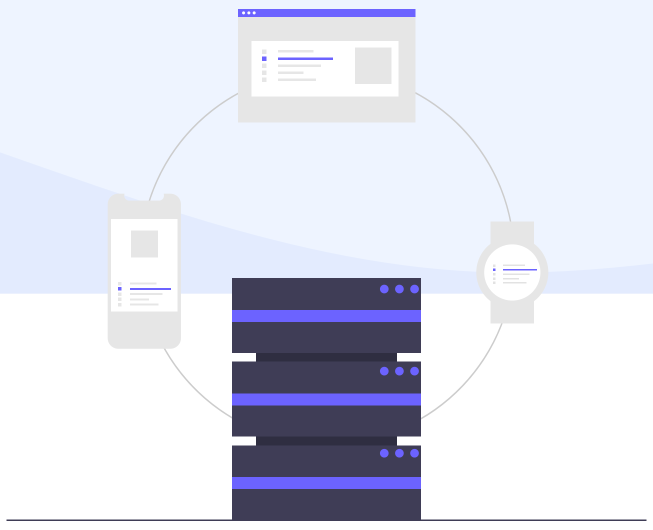
07



Calendar phishing

Calendar phishing involves sending fake calendar invitations with phishing links. These invitations often mimic common event requests and can easily be added to calendars automatically.

08



Pharming

Pharming is a highly technical form of phishing, making it harder to detect. It involves a hacker hijacking the DNS (Domain Name Server), which converts URLs from plain language to IP addresses. When users enter the target website's URL, the DNS redirects them to another IP address, usually of a malicious website that appears legitimate.

09

iq.global/phishing