# Understanding Clickjacking: The Browser-Based Attack That Can Bypass Protections to Take Over Accounts

Clickjacking tricks unsuspecting people into clicking on links they think are harmless — but then downloads malware, harvests login credentials, and takes over online accounts.

Clickjacking tricks unsuspecting people into clicking on links that they think are harmless — but then download malware, harvest login credentials, and take over online accounts. Unfortunately, clickjacking malware can evade security protections, but there are ways to protect yourself.

1. From DNS vulnerabilities to clickjacking

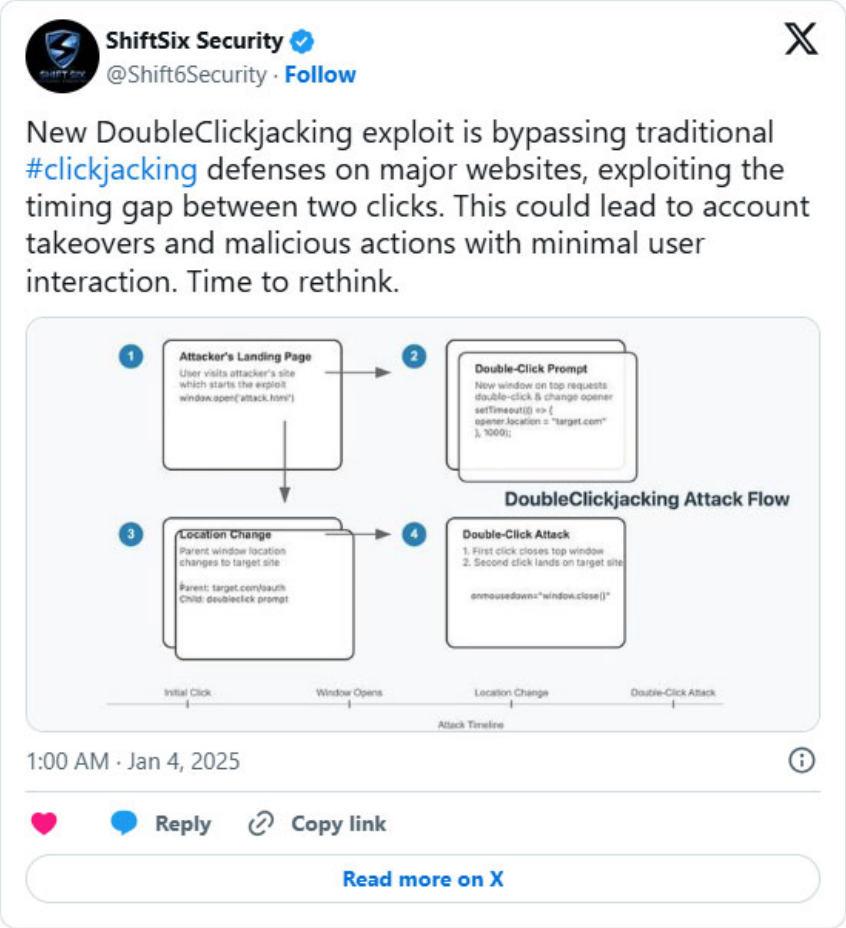
## What is Clickjacking?

Also known as UI redress attack, clickjacking is a form of interface-based attack that manipulates users into clicking on buttons or links that are disguised as something else.

Unlike phishing, where the victim is taken to a fake website designed to mimic a legitimate company's website, clickjacking takes the user to the real website. However, the attacker creates an invisible overlay on top of the legitimate website using HTML tools such as cascading style sheets (CSS) and iframes.

The invisible layer is created using an iframe, an HTML element used to embed a web page or HTML document into another web page. It is transparent, so it still looks like you are interacting with a legitimate website. However, if you click on a button on the website, play a game, or perform a task that you think is harmless, those clicks are applied to the invisible web page at the top. These clicks give hackers access to your account, allowing them to download malware, take control of your device, and perform other nefarious activities.

Sometimes, attackers disguise themselves as marketers and trick users into liking a social media page or post. This attack is called likejacking. The attacker sends the user an interesting video or 'special offer,' and when the user clicks 'Play' or interacts with the content, they accidentally click the hidden like button.




Another version of clickjacking, called cursor-jacking, tricks users with a custom cursor into clicking on links or parts of a website that the user did not intend to interact with.

A more advanced variation of clickjacking called double clickjacking exploits the timing and sequence of users' double clicks.

## Bypass antivirus and browser protection

What makes people worried about clickjacking is that it often bypasses antivirus and antimalware software. Because these attacks occur on reputable websites and don't always involve downloading anything, traditional antivirus software may not detect them.

Most browsers have built-in protections, but as we all know, hackers are always looking for new ways to exploit users online. Most basic clickjacking attacks are effectively blocked – but not double clickjacking attacks.

Instead of something malicious happening on your first click, the attacker's code will insert a hijacked overlay before prompting you to click a second time. This could appear as a simple double-click to confirm the action or a nasty CAPTCHA. On the second click, you could accidentally install a plugin and give the attacker access to your account.


Currently, browsers may not detect this more sophisticated version because it doesn't use the usual iframe setup, leaving you at a higher risk of being a victim of clickjacking. This isn't limited to desktop browsers; mobile users are also targeted with double-tap prompts.

## How Doublejacking Bypasses Clickjacking Protections

Many modern web browsers have built-in security protections to mitigate clickjacking. However, a sophisticated version called 'double clickjacking' can bypass traditional protections by exploiting the sequence between two clicks to take over accounts or perform unauthorized actions.

In a double clickjacking attack, malicious elements are inserted between the user's first and second clicks. First, you are taken to an attacker-controlled website and presented with a prompt, such as solving a CAPTCHA or double-clicking a button to authorize an action. The first click closes or changes the top window (overlay CAPTCHA), causing the second click to go to the previously hidden authorization button or link. The second click authorizes malicious plugins, causing the OAuth application to connect to your account or approve a multi-factor authentication prompt.

## What you can do to protect yourself

Clickjacking techniques are sophisticated and designed to trick and steal your clicks, but there are a few things you can do to protect yourself.

1. Keep your devices and browsers up to date. Pay attention to security patches and software updates and install them as soon as they become available. Engineers regularly release patches to address security vulnerabilities and protect users from new attacks.
2. Be suspicious of double-click prompts, especially on websites you're unfamiliar with.
3. Always double-check the URLs of the websites you visit. Attackers can use typosquatting techniques to purchase legitimate versions of domains that have very slight differences, such as adding an "a" or a hyphen to the domain, such as "ama-zon.com".

4. Avoid clicking on links when you are unsure of the source. You can use a website link checker to see if the link is safe.

Attackers often take advantage of your trust in legitimate websites and basic actions we often do without thinking, like double-clicking. Always slow down and think before you click to protect yourself.