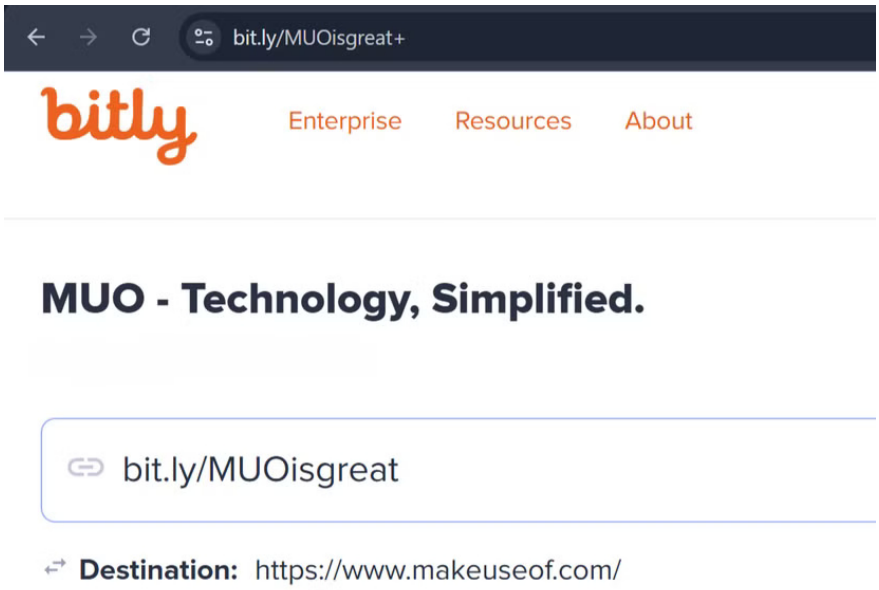
Do not click on any shortened link until you are sure it is safe!

Shortened URLs are convenient for cleaning up long links, but they also hide the real destination. If you want to avoid malware or phishing, blindly clicking on that link is not a wise choice.

Shortened URLs are great for cleaning up long links, but they also hide the real destination. If you want to avoid malware or phishing, blindly clicking on that link isn't a good idea - there are better, safer options!

Why are shortened URLs a security nightmare?

The biggest problem with shortened URLs is simple: you can't see the destination. A neat, clean link from a service like Bitly or TinyURL completely obscures the actual web address you're about to visit. It's a complete blind spot in online safety, leaving you 100% trusting the sender.



Attackers love this lack of transparency. They can hide a malicious domain behind a trusted shortener to do phishing. These are email habits that hackers use to target you—luring you with a link that looks clean but leads to a fake login page designed to steal your credentials.

Just one click can trigger an automated download, where malware is automatically installed on your device. You don't even have to click anything on the malicious page. This makes it important to know how to check if a downloaded file is safe before it's too late.

Worse yet, scammers can customize shortened links to look more legitimate (e.g., Bit.ly/courier-tracking-update). This social engineering tactic plays on your trust and sense of urgency. The same convenience that makes shortened URLs so popular is what makes them a security nightmare—they encourage you to click first and think later.

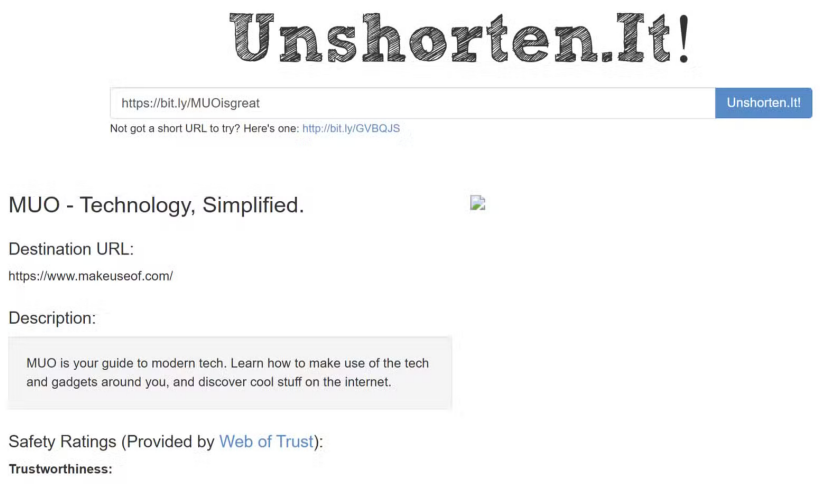
How to open shortened URL safely

You don't have to play Russian roulette with every shortened link you see. With the right approach, you can expose these URLs and check their destination before you even think about clicking. It's a two-step process: First, expand, then scan.

Expand URL without clicking

Instead of clicking randomly, take a moment to reveal the true destination of a link. The best way to do this is to use a URL expander — a simple web tool that shows you the full address.

Just copy the shortened link and paste it into a site like Unshorten.it or CheckShortURL . These services will automatically redirect and show you the final URL. It's a quick, easy step that takes the guesswork out of clicking.



Some URL shorteners offer built-in ways to preview the destination without clicking. For Bitly links, just add a '+' symbol to the end of the URL to see where it leads. TinyURL lets you add a 'preview' before your shortened link for a secure preview page. These quick tips work directly in your browser without any third-party tools.

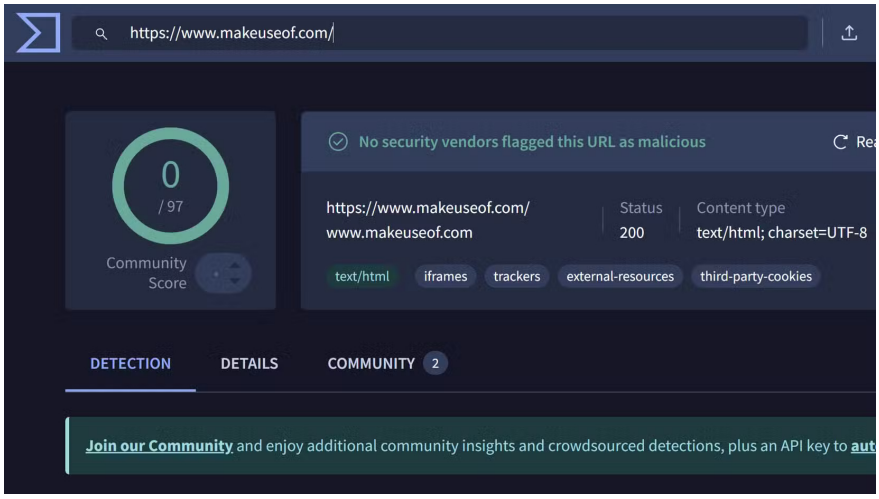
Once the full URL is displayed, double-check it. Is the domain correct? A link that is supposed to be for delivery shouldn't lead to a strange, unrelated site. Look for fake domains that mimic real domains, a classic tactic in scams.

Also, check for suspicious file extensions at the end of the URL, such as .exe or .zip. A link that immediately attempts to download a file is a serious warning sign.

Run a quick virus scan

Even if the extension URL looks legitimate, you should still get a second opinion. The site itself could be compromised. This is where online security scanners come in; they analyze landing pages for known threats.

Services like VirusTotal and URLVoid are great for this. Paste the full URL extension into the search bar, and the service will check it against dozens of antivirus engines and blocklists. The report will tell you whether any security vendors have flagged the site as malicious. This process gives you a comprehensive threat assessment in just a few seconds.



You finished reading the article "**Do not click on any shortened link until you are sure it is safe!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.