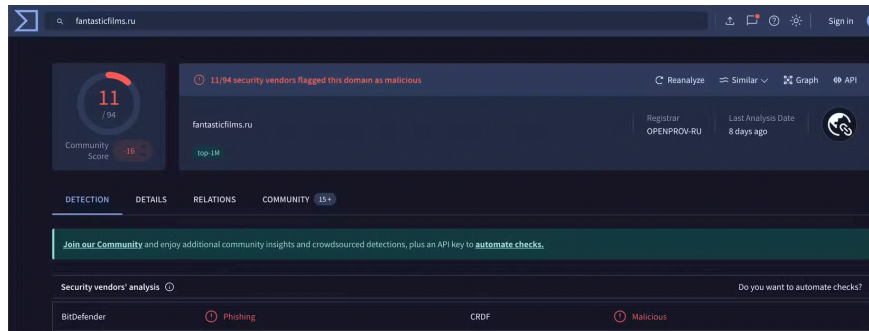


4 tools to detect phishing emails

Email phishing is no longer as simple as it used to be. Scammers are now tech-savvy criminals who leverage advanced tools to scam victims.

Email phishing isn't as simple as it used to be. Scammers are now tech-savvy criminals who use advanced tools to trick their victims. But they're not the only ones with an arsenal of tools at their disposal.

1. VirusTotal

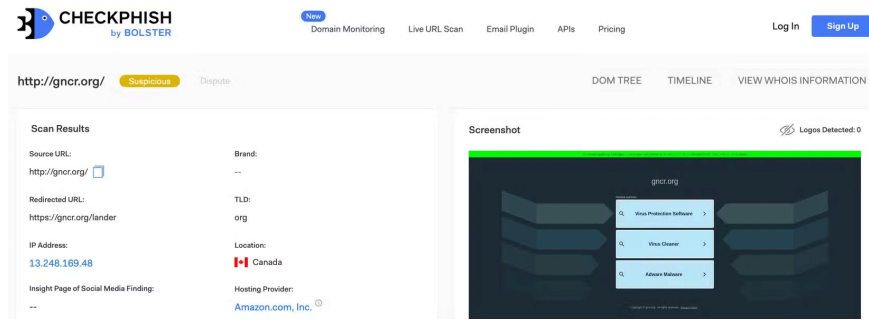


Most phishing emails will send you files and links attached or try to take you to a website. How do you know if these files, links, and websites are safe?

One way to find out is to run them through VirusTotal's malware scanner. When run through VirusTotal's free detection feature, over 70 antivirus scanners and URL/domain blocking services will analyze your file, link, or website.

After running the scanner, you'll be presented with results from your antivirus scanner, indicating whether the link, file, or domain you entered is considered clean or some form of malware. For example, a VirusTotal scan of 17ebook.com shows that some sites consider it malicious, malware, or phishing, so you should probably avoid it.

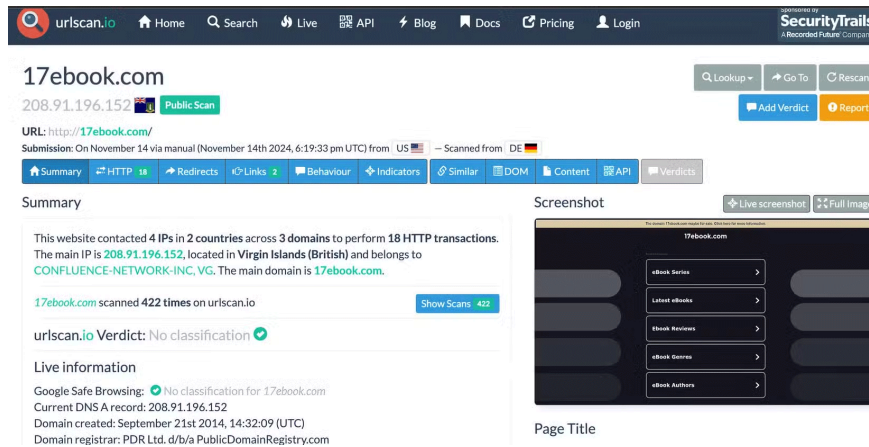
2. CheckPhish



Before clicking on a link that takes you to an unknown website, make sure to run it through a website scanner like CheckPhish. CheckPhish scans suspicious websites to determine if they are malicious. After scanning a website, you'll be notified if it's clean, suspicious, or a known threat. You'll also learn information like the site's IP location, hosting provider, certificate details, related URLs, and phishing history.

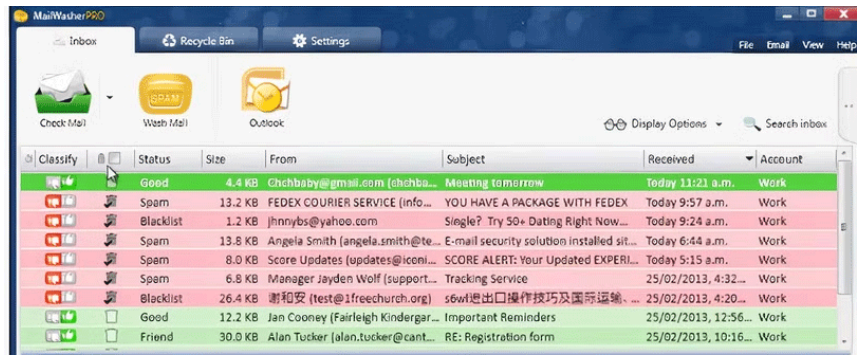
CheckPhish will also warn you if the URL in question is a typosquatting site. A typosquatting site is a site that mimics a legitimate site but is designed with malicious intent. These sites are usually one or two characters different from the more popular sites. Once you visit, you may not know you're on the wrong site because the mimicking domain is similar to the site you're trying to access.

3. urlscan.io



urlscan.io is only used to analyze websites for malware. After the scan, you will receive a verdict of whether the website is safe/unsafe or unknown. You will also be provided with a screenshot of the website, DNS and IP records, and the platform the website is hosted on.

4. Mailwasher



Regardless of your email client, it will most likely filter out phishing, spam, and junk emails. But that doesn't necessarily mean that downloading a spam blocker like Mailwasher is unnecessary. Cybersecurity experts believe in a concept called defense in depth, which means that multiple layers of security create a strong digital defense. Using Mailwasher in conjunction with the built-in spam filter used by your email client will only increase your security.

Mailwasher can detect spam, phishing emails, viruses, and even unwanted newsletters and emails. It's not a browser plug-in that runs in the background when you open your mail client. Instead, you have to connect your email to MailWasher and run the program to check your emails. If you suspect an email, you can preview it without opening it. If the program judges the email as malicious, you can delete it from within the program itself.

Scammers may have evolved in recent years, but they aren't the only ones who can leverage the latest tools to their advantage.

You finished reading the article "**4 tools to detect phishing emails**" 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.