TARGETED PHISHING RESOURCES:

Here are some other great links for apps / websites that will make you MUCH more prepared to deal with phishing and social engineering attacks. Please spend some time becoming familiar with them, installing them and/or bookmarking them for future reference.

Trust me they are AWESOME!

- https://phishingquiz.withgoogle.com/
  - Please try this quick email phishing simulation created by Google themselves! They present you with 8 VERY realistic emails, and you might be surprised by how sneaky these phishing emails can be. Good luck!

- https://beinternetawesome.withgoogle.com/en_us/interland/landing/reality-river
  - Very cool! Google has created an online game called **Interland: Reality River,** in which kids have to answer certain questions to cross and avoid the phishers :)

- https://unshorten.link/
- https://chrome.google.com/webstore/detail/unshortenlink/gbob-daaeaihkghbokihkofcbndhmbdpd?hl=en
  - If you receive a shortened URL (in an email for instance), you can copy/paste the URL into this website and it will show you the full-length website URL, so you see where it really points to. They also have a Chrome extension that does similar analysis

- https://www.virustotal.com/#/home/url
    - VirusTotal is a free service that will either scan a website link, and tell you if it is malicious. Or, if you have received a file that you do not trust, you can scan it against 70 major antivirus scanners to tell you if it sees anything suspicious

- https://tech.firstlook.media/dangerzone-working-with-suspicious-documents-without-getting-hacked
    - A wonderful new tool called **DangerZone** that's been released that allows you to open any document receive, and strip out anything malicious from inside it. Takes a few things to set it up, but then it's all worth it

- https://transparencyreport.google.com/safe-browsing/search
    - To quickly check if a website or a specific URL is safe to visit, please paste the website link into Google Safe Browsing website checker

- https://www.malwarebytes.com/mobile/
    - MalwareBytes has a great mobile app for iOS/Android that will warn you about malware, phishing sites and scam calls/texts you do not trust

- https://www.bitdefender.com/solutions/trafficlight.html
    - BitDefender has a great browser add-on that will detect malware, phishing attacks, as well as a website link scanner

- https://toolbar.netcraft.com/
    - Netcraft's browser add-on uses crowdsourced data to tell you about a website's reputation, warn you about visiting phishing sites, and exposure to malware

- https://chrome.google.com/webstore/detail/windows-defender-browser/bkbeeeffjjeopflfhgeknacdieedcoml

    - Microsoft's respected SmartScreen Filter was ported over so you can use it as a Chrome extension called Windows Defender Browser

- https://www.geckoandfly.com/25017/security-toolbar-phishing-web-sites/
    - A good list of anti-phishing browser add-ons you can install for extra protection when you browse

- https://www.mcafee.com/consumer/en-us/store/m0/catalog/mwad_528/mcafee-web-advisor.html
    - McAfee WebAdvisor is a free download that will warn you if you visit malicious websites, and/or download malicious files.

- http://db.aa419.org/fakebankslist.php
    - An interesting website that aggregates many of the websites used in fake bank and lottery websites into a searchable data-base

==

Lenny Zeltser (a famed malware researcher), has an incredible compiled list of the most popular website URL/file scanners you can use, to scan website URL's to see if they are malicious before you visit them. Definitely bookmark this page! It's **VERY** worthwhile going through the list and bookmarking. Here is the link:

https://zeltser.com/lookup-malicious-websites/

Keep in mind that some of these tools will provide historical information about the website, e.g. how long it has been up, where it is located and so on, and others will examine the website URL in real time and let you know if it sees anything malicious.

Both bits of information can help you decide whether you should visit a certain website or not, so please keep them handy.

Here are some on that list and a few extra that you should definitely bookmark and use, as they all provide great value for free:

Free Online Tools for Looking up Potentially Malicious Websites

Please refer to these links whenever you **receive an email with a suspicious link**, or a **file you absolutely do not want to open**, but want to safely analyze off your system to see if it is malicious (**without clicking any links in the email** - hover your mouse over the embedded link - right click to pull up the context menu - choose "Copy Link Location" and paste the contents into one of these scanners):

https://urlquery.net/
https://www.urlvoid.com/
https://www.mywot.com/
https://global.sitesafety.trendmicro.com/
https://safeweb.norton.com/
https://trustedsource.org/sources/index.pl
https://www.brightcloud.com/tools/url-ip-lookup.php
https://app.webinspector.com/
https://checkphish.ai/
http://www.unmaskparasites.com/
https://global.sitesafety.trendmicro.com/
http://onlinelinkscan.com/
https://www.f-secure.com/en_US/web/home_us/online-scanner
http://www.unmaskparasites.com/security-report/
https://www.phishtank.com/
http://vurl.mysteryfcm.co.uk/

https://www.joesandbox.com/

Joe Sandbox is great if you want to geek out a bit and see what's really going on under the hood, so to speak. It "detects and analyzes potential malicious files and URLs on Windows, Android, Mac OS, Linux, and iOS for suspicious activities. It performs deep malware analysis and generates comprehensive and detailed analysis reports."