Endeavour Foundation

Edition 4

SECURITY HINTS & TIPS: Shortened Links

What Are Shortened Links? Have you ever clicked a link only to be redirected to another link with a longer URL? If so, you probably clicked a shortened link. URL shortening occurs when a URL is swapped out for a shorter link that redirects you back to the original link. Shortened links first appeared in the early 2000s but became more popular with the rise of Twitter. Today, shortened links are commonly used to track marketing and social media campaigns.

How Do Cybercriminals Use Shortened Links?

Unfortunately, cybercriminals discovered that shortened links can make malicious links look safe to click. Shortened links hide the real URL, and many URL shorteners also change the domain when generating a shortened link. Since the real URL isn't visible, users can't see the red flags that might prevent them from clicking a link.

For example, cybercriminals repurposed LinkedIn redirect links, or "slinks", to steal users' credentials. Slinks are typically used to track marketing campaigns on LinkedIn while also letting companies link out to their websites. Since all slinks use the LinkedIn domain, they are unlikely to be blocked by anti-spam or anti-malware filters. Users are also more likely to click slinks because LinkedIn is a trusted website. Cybercriminals use slinks to redirect users to a fake login page and then steal any credentials the users enter on the page.

Hints and Tips to Stay Safe

- Always think before you click! Remember that you should never click a link that you weren't expecting.
- Become familiar with popular URL shortener tools. For example, Bitly and TinyURL are two common URL shorteners. If you see a link with Bitly or TinyURL at the beginning of the link, you can assume the link has been shortened.
- If you suspect a link has been shortened, use a link expander to view the full URL before you click. Expanding the URL will help you identify any potential red flags.

Stop, Look, and Think. Don't be fooled.