Keenan FIRESTORM GLOBAL

Safe Web Browsing

MONTHLY CYBERSECURITY BYTES

Today, the average internet user spends over 6 hours per day online during which we navigate the web by browsing, clicking, and downloading across myriad devices. While most of these activities are benign, it only takes one wrong move to fall victim to a malicious scam. Nearly one-third of all malware infections stem from internet use and 68% of all data breaches originate with human error. Cybercriminals have long recognized that it's generally easier to trick susceptible humans rather than hacking computer systems. The good news is that by following a few simple safe browsing practices, you can greatly reduce these risks and keep both your personal and organizational data safer.

Avoid Unsafe Downloads

One of the easiest ways to get malware is by downloading untrusted files. Only download software, documents or media from official websites or reputable vendors and be cautious of freeware sites or pop-ups urging you to download something. Use your endpoint protection software to scan downloads and attachments. If you notice anything unexpected after downloading a file, contact your IT department.

Fill Out Forms Cautiously

Forms are an easy way for cybercriminals to capture sensitive information by impersonating trusted sources. Verify authenticity before filling out any form and exercise extreme caution before sharing personal information. Never share your password in an online form even if it appears to be a trusted source. For example, threat actors often use common tools like Google Forms to impersonate IT and request system passwords.

Steer Clear of Phishing Sites

Review the URL (e.g., www.google.com) carefully, especially if you arrived at a site by clicking on a link from a text, email or other website. When in doubt, search for the name of the trusted service and compare that to what's shown in your browser. Savvy cybercriminals may copy a trusted website's design to resemble the legitimate site, using a similar URL. They will then capture your login credentials and attempt to reuse them elsewhere. For anything sensitive, go directly to the trusted site and navigate to the appropriate section rather than clicking a link.

Redirects

Redirects are common among legitimate sites, where a shorter URL is provided instead of the actual final URL. This technique allows the site to better track you and provide a more convenient link to click. It's important to note that bad actors are aware of this method as well and often use "link shorteners" to hide the malicious final destination.

Update Software

Updating software is a consistent best practice in information security. Outdated, unpatched software can be vulnerable allowing hackers to exploit known weaknesses. When updates become available, take a moment to apply them or use your device's "install tonight" feature to help keep devices protected.

By incorporating these safe browsing practices into your daily routine, you'll reduce the risk of falling for online scams and help protect both personal and organizational data.

Cybersecurity Questions?

Members receive advanced cybersecurity support at no additional cost including access to cybersecurity risk assessments, cyber awareness resources, external risk analysis, "ask an expert" help line and more.

If you have questions or would like to learn more, contact support@firestormglobal.com.