National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

The Suffering Surfer

In the early days of computers, malware was a prank to annoy people and show off programming skills. Today, the driving force is money, and as a result, malware is everywhere!

We've learned to not download unfamiliar email attachments and to avoid file-sharing services because you just can't trust files these days. One thing we haven't stopped doing, though, is surfing the web.

Consequently, websites have become a primary instrument for dirty rotten malware mongers. In fact, Google blacklists about 6,000 websites a day for hosting some sort of malicious software. Unfortunately, many of these websites are victims themselves, hosting adware and other unsavory content without even knowing it!

It's not just adult and gossip sites anymore, either. Legitimate websites like Huffington Post, LA Weekly, and the US Army's public website were compromised in 2015, some hosting malware that infected their visitors.

The IHS network actively scans for malware and blocks malicious websites, but home networks may not be safe. Governement equipment could be at risk while teleworking.

The Malvertising Menace

One of the most prevalant website swindles is malvertising - malicious advertisements that automatically redirect victims to a bogus page, which silently attacks their computers and installs malware.

How does it work?

Criminals run ads through unwitting online advertising companies. The ads appear on associated webpages, tempting visitors with shocking slideshows, amazing deals, or tantalyzing content. When the user clicks on the ad, it redirects them through several domains before finally dumping them onto a page hosting an exploit kit. Here, their computer is scanned for vulnerabilities, and when one is found (like unpatched or outdated software), malware is automatically delivered.

How does it deliver?

A website might trick the visitor into downloading the code - like telling the user they must download a particular software in order to view a video. Or a banner ad might initiate a download just on a user's curious click.

But most troubling are the ***drive-by downloads.*** They require no action at all. The suffering surfer only has to visit the page to kick off malware hidden inside invisible elements or embedded in images, videos, or Flash animations.

The impervious iOS?

Don't go thinking just because you have a Mac you're safe from malware. Blogging applications like WordPress have made site development simple and multi-media rich for 50 million websites. They've also been the conduit for assaulting 500,000 Macs with a Trojan-infected plug-in.

National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

The Suffering Surfer

Malvertized and Scandalized?

In some cases, visiting a website will initiate phony software update prompts. The example at the top-left is a fake Adobe update. The user is told they *must* install, and the window won't go away until they agree to do so.

Other victims are fooled by option buttons to "Install Later," which actually kick off the install just the same. Always click the X to close out the dialog box if given the choice.

The Mac virus warning at the bottom-left claims the computer has been hacked and the user must contact emergency support immediately. But that "tech support" is a scammer. The cleanup program they'll sell you is a scam too! Lots of alleged anti-malware programs are scams that put your system at even higher risk of exploitation.

If closing the browser makes the window disappear, it's probably due to adware. But what do you do if the window pops back up each time you open the browser?

Exorcising Malvertising

If your personal equipment has been victimized, there are things you can do to counteract the damage.

Uninstall the dirty rotten program!

In Windows, go to the **Control Panel** and click on **Progams and Features**. Scroll through the list of programs and look for the ones that were recently installed. You might find dozens that were installed on the same day! Look for unwanted or unknown programs with names like PriceMeter, Zombie Alert, Trusted Web, TidyNetwork, or BlockAndSurf.

Remove those dirty rotten browser plug-ins!

Reset your browser settings. In Internet Explorer, use the gear icon in the top-right of your browser, and to the **Internet Options > Advanced > Reset**. Check the **Delete personal settings box** and click **Reset**. Other browsers have similar reset functions.

Disable that jerky Java!

Block Java where possible, using browser settings or a program like Noscript.

Let loose the awesome power of really smart software developers!

Several adware removal and anti-malware products are available for use on personal equipment... some even offer free downloads, like www.Malwarebytes.org. Folks may say, "you get what you pay for," but others will tout the benefits of freeware. Don't be fooled by cheap but crooked cure-alls. Research user reviews to find your best solution!

By using these tips, you can become a SAVVY SURFER!