PROJECT CYBERSAFE™

NEWSLETTER

A QUARTERLY PUBLICATION FOR NSSF AND SAAMI EMPLOYEES

PHISHING SEASON NEVER ENDS, AND NO LICENSE IS NEEDED.

Phishing continues to be the top method of cyber-attack. Hacking groups are now creating Phishing As A Service software that is giving this capability to bad actors that lack the technical sophistication that used to be required to conduct such wide-scale attacks.

Cybercriminals continue to create attacks that avoid detection and have started to increase the number of attacks on mobile devices. In the recently released Comcast Business 2024 Cybersecurity Threat Report, 2.6 billion phishing events were detected by Comcast Business last year. To put that big a number into perspective, that is slightly less than 5000 phishing attacks detected every minute of last year. And that is just for the customers that Comcast monitors. These numbers line up similarly to other security vendors and spotlight the need to stay vigilant and up to date on the new techniques cyber criminals are using against the public. KnowBe4 breaks down the article here.

FILE TYPES AVOIDING SECURITY DETECTION

There are a variety of file attachments that are not common for legitimate emails that are avoiding email security and should be treated with suspicion.

The normal file types we all deal with are DOC or DOCX, XLS or XLSX or CSV or PDF. You may also get image files such as JPG or PNG.

The best advice I can provide is **Be very wary of any file types outside of those attachments you regularly interact with, unless you explicitly expect other types of files from vendors or our members.**

Threat actors are increasingly using Scalable Vector Graphics (SVG) attachments to display phishing forms or deploy malware while evading detection.

Most images on the web are JPG or PNG files, which are made of grids of tiny squares called pixels. Each pixel has a specific color value, and together, these pixels form the entire image.

SVG, or Scalable Vector Graphics, displays images differently, as instead of using pixels, the images are created through lines, shapes, and text described in textual mathematical formulas in the code.

Threat actors are increasingly using SVG files in their phishing campaigns according to security researcher MalwareHunterTeam.

The problem is that since these files are mostly just textual representations of images, they tend not to be detected by security software that often. From samples seen by BleepingComputer and uploaded to VirusTotal, at the most, they have one or two detections by security software.

With that said, receiving an SVG attachment is not common for legitimate emails, and should immediately be treated with suspicion. Unless you are a developer and expect to receive these types of attachments, it is safer to delete any emails containing them. Read the full article.

A PROGRAM OF NSSF® The Firearm Industry Trade Association

UPDATE! DAISY, THE AI GRANNY WASTING SCAMMERS' TIME

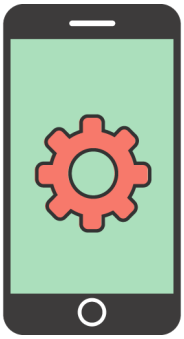
For those who may not have seen the link I shared in the RingCentral Watercooler, a recent NPR story talked about O2's Daisy the AI Granny wasting scammers time. The NPR 2-minute listen reports that "Scammers stole an estimated $1 TRILLION dollars from people who gave out their personal information according to the Global Anti-Scam Alliance." If you want to actually see Daisy in action you can visit the O2 website here.

UK company, Virgin Media O2, has unveiled the newest member of its fraud prevention team, 'Daisy'. As 'Head of Scammer Relations', this state-of-the-art AI Granny's mission is to talk with fraudsters and waste as much of their time as possible with human-like rambling chat to keep them away from real people, while highlighting the need for consumers to stay vigilant as the UK faces a fraud epidemic.

HOME SMART DEVICES: APP PERMISSION SETTINGS

With new smart devices come more apps on your phone. From Robot vacuums to smart cameras to latest kids toys, all these Apps at a minimum want to know your location for the purposes of marketing and selling that data. Some apps, as innocuous as they may seem, want access to your camera, microphone, and contacts. You can control the level of access these Apps have by going through each one individually and disabling these settings.

SAFE TRAVELS



Please take this week to ensure your iPhone and iPad are updated to Apple iOS 18.2.

Turning OFF Bluetooth and Wi-Fi whenever possible can save battery power. This also limits the ability to accidentally connect to an unwanted network or device searching for other devices to connect to. Dimming your screen light can also preserve battery if you find yourself running low.

Take a moment to read the tips on the next page, especially the tip about using your phone as a hotspot to avoid using public Wi-Fi.

KIDS CORNER

Bark was created by a father of 2 boys, and it has a wealth of articles that can assist in setting boundaries and starting the tech conversations needed with your children. He also has phones and watches that have built-in parental controls. Check out the Bark blog.

NATIONAL CYBERSECURITY ALLIANCE

TOP 5 CYBER SAFETY TIPS FOR TRAVELERS

These days, no matter where you're headed, being continuously connected is part of the travel plan. As you embark on your next adventure, the National Cyber Security Alliance (NCSA) urges travelers to stay cyber safe while away from home by following some simple practices to help keep your devices safe and your vacation plans from going awry.

1. Set up the "find my phone" feature on your devices

Before you head out on vacation, this setting will allow you to find, remotely wipe data and/or disable the device if it gets into the wrong hands.

2. If you share computers, don't share information

Be extremely cautious on public computers in airports, hotel lobbies and internet cafes. Keep activities as generic and anonymous as possible. If you do log into accounts, such as email, always click "logout" when you are finished. Simply clicking the "x" does not log you out of accounts.

3. Get savvy about WiFi hotspots

Do not transmit personal info or make purchases on unsecure networks. Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

4. Protect Physical Devices

Ensure your devices are with you at all times. If you are staying in a hotel, the best thing to do is lock them in a safe or lock them in your luggage.

Using your device at an airport or cafe? Don't leave it unattended with a stranger while you get up to use the restroom or order another latte. Keep your devices with you at all times. The phrase "stranger danger" also applies to cybersecurity.

5. Actively manage location services

Location tools come in handy while planning navigating a new place, but they can also expose your location – even through photos. Turn off location services when not in use.

STAYSAFEONLINE.ORG
@STAYSAFEONLINE
/STAYSAFEONLINE