Freedman Consulting, Inc.
CHANGE . . . RESULTS . . . SUCCESS

THOSE VEXING NOTIFICATIONS

Ellen Freedman, CLM

I'm sure it will not surprise my readers – knowing I'm a belt & suspenders type of gal – that I maintain a folder labeled "future article ideas." I rarely have to reach into this folder. Thankfully, the ever-ringing hotline usually provides me with more than ample situations from which I can develop articles. However, as the deadline for this issue's column crept closer, it became increasingly apparent that this might be the first time in a long time for me to reach for the folder.

I had a surprising accumulation of topic areas included in the folder. Most were older and not really of interest nowadays. Then I spotted one item from early 2023 that caught my attention. A solo Pittsburgh attorney emailed me the topic idea and asked me to write about it. To my delight, it is relevant, and something you all should know about. A tip of the hat to the attorney who sent me this topic.

Many of us struggle with – or are at least annoyed by – computer pop-up notifications. These notifications always seem to pop up out of nowhere when we are distracted and rushed with deadlines. Our immediate response is annoyance, followed instantly by a desire to get rid of them as quickly as possible.

Let's be honest, though. We are simultaneously wondering – most of the time, based on the message content – whether it is legitimate or a scam. And if it's a scam, we are wondering how it got past our security defenses.

You're not being paranoid. Well, maybe you *are* paranoid, but that doesn't mean people aren't actually out to get you! Today's reality is that browser notification scams and fake security pop-ups are frequently used as initial social engineering tools that can lead to credential theft, remote-access compromise, malware installation and ultimately data breaches or financial fraud.

The browser-based scams circulating today are especially dangerous because they often exploit legitimate browser notification features that allow them to bypass

traditional antivirus detection. Once they reach your desktop, all they have to do is sufficiently deceive you (scare you?) into performing some action.

Our web browsers allow the websites we visit to ask permission to send notifications. Legitimate websites use this feature to send you updates, calendar reminders, news alerts or messages. We frequently click "allow" to enable these features.

Cybercriminals abuse this system by tricking users into clicking "allow" on deceptive prompts. Examples of deceptive prompts include things like:

- "Click allow to confirm you are not a robot"
- "Enable notifications to continue"
- "Click allow to watch the video"
- "Your download is ready, click allow to continue"

Once permission is granted, the browser begins displaying pop-up notifications directly on the user's desktop, even when the browser itself is closed. Even after a reboot. Even after you've run a full antivirus and antimalware scan of your computer. Because notifications are delivered through approved functionality and no malicious file has been installed on your computer, they do not get classified as malicious by your security software.

The pop-up alerts frequently impersonate trusted companies such as Microsoft, Apple, McAfee or Norton or your IT support company. I sometimes get one that appears to come from my own tech-support department at Freedman Consulting. Fortunately, I know that is me! The notifications frequently imitate legitimate security warnings, with claims like:

- The computer is infected
- A subscription has expired
- A password has expired
- Files are compromised
- Immediate action is required

These scams rely on deception and psychological pressure. What you face is sophisticated social engineering, rather than malware. The criminal's objective is to persuade you to take harmful action voluntarily. The biggest and sometimes *only* "tell" that the pop-up is a scam is the urgency it creates for you to act immediately, before it is too late.

"Hey, Ellen, what about the "black list" that is provided by my security software? I add to it all the time when I identify a new malicious domain. Doesn't that protect me? "

Unfortunately, no. Fraudulent notification websites appear and disappear rapidly. With the use of AI to support new domain registrations and new scam websites that can look identical to a legitimate one except for one letter in the domain URL, even highly sophisticated AI-powered security products may not recognize a newly created malicious site immediately.

I will not take advantage of this opportunity to tell you why law firms are attractive targets. I have written about this and spoken at webinars and seminars about this countless times. If you don't know by now that every law firm – solo to megasize – overflows with exactly the type of information and ready-to-grab money criminals hunger for, nothing I say at this point will convince you.

Instead, I will give you a bit of good news. These attacks are often reversable if addressed quickly, before you click on anything in a pop-up that will make things worse. Much worse. No, stop that, put your hand in your lap! Do not click on anything in that pop-up, other than the close button, if it has one. If it doesn't, reboot your computer. Then follow the directions below for whatever browser(s) you use to stop additional malicious browser notifications.

Google Chrome 1.
Open Settings.
2. Select "Privacy and Security."
3. Choose "Site Settings."
4. Click "Notifications."
5. Remove suspicious or unfamiliar websites from the "Allowed" list.

Microsoft Edge 1.
Open Settings.
2. Select "Cookies and Site Permissions."
3. Choose "Notifications."
4. Remove unknown or suspicious sites.

Mozilla Firefox 1.
Open Settings.
2. Select "Privacy & Security."
3. Locate "Permissions."
4. Review notification settings and remove unknown or suspicious sites.

Apple Safari
1. Open Safari Settings. 2.
Select "Websites."

3. Click "Notifications."
4. Deny or remove suspicious permissions.

All users (regardless of browser) should then:

1. Clear browser cache and cookies.
2. Run a reputable malware scan.
3. Update browsers and operating systems (if they are not the current version).
4. Restart your device (note that all devices are vulnerable, including phones).

There are a few related best practices for law firms. These include providing security awareness training, limiting administrative privileges of end-users, centrally managing browser settings to block or limit notification permissions and using multiple layers of security such as multi-factor authentication and endpoint detection and response (EDR).

One final but important suggestion is to enable employees to feel comfortable reporting suspicious pop-ups without fear of criticism. If they're afraid of you killing the messenger, they might try to deal with it on their own. Bad decision. Very bad decision.

In closing, I thought I would remind you about one early pop-up scam that cost millions and corrupted many computers beyond repair. I was one of the victims. It involved fake pop-up security alerts. Here's the article about it on the FTC website: "FTC Charges Tech Support Companies With Using Deceptive Pop-Up Ads to Scare Consumers Into Purchasing Unneeded Services." PBA members who want to read about my personal experience with this scam can send an email request for my article "I've Been Infected!" I'm not ashamed to admit I was a victim.

A version of this article originally appeared in the June 15, 2026 issue of Pennsylvania Bar News.