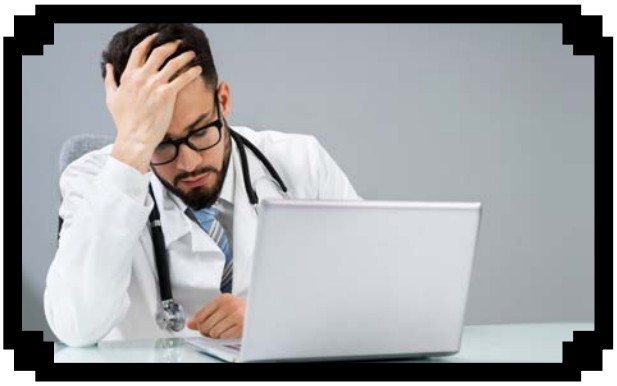
What is Scareware?

Office of Information Technology
Division of Information Security
MAY 2024



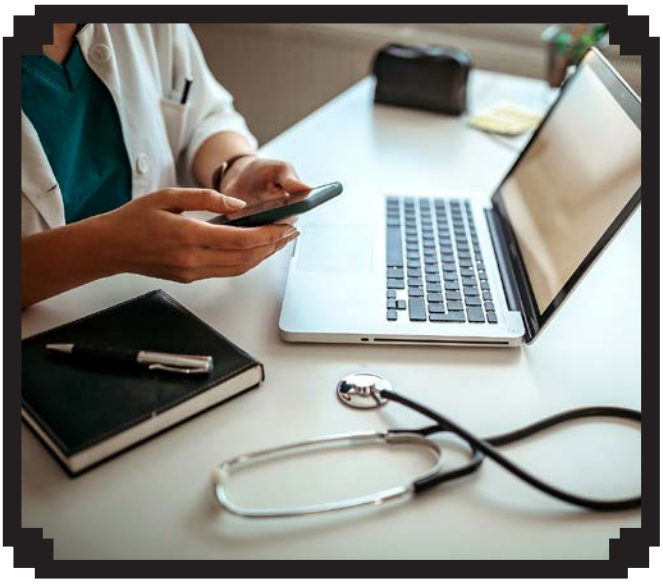
Scareware is a type of malware that leverages pop-up ads and social engineering techniques on a user's device. Scareware urges the user to act quickly to "fix" a cybersecurity problem. The software promoted is not needed and is instead often malicious. As the name suggests, scareware scares the user into providing sensitive data such as usernames, passwords, or credit card information to purchase and install unneeded software. Once that purchase is complete, an attacker may further exploit the confidential information the user provided against the user, resulting in identity theft or credit card fraud.

Recent data indicates that scareware continues to be a significant threat to computer users worldwide:

- The Anti-Phishing Working Group observed a substantial rise in scareware packages circulating online. In the second half of 2023, the number of scareware packages surged from 12,500 to 21,800, marking a concerning 74% increase.
- In terms of financial impact, 2023 scareware incidents resulted in over $200 million in global losses, with individual victims averaging a loss of $600 per incident.
- Scareware reports have increased in recent years, with users encountering the following alarming sequence of events:

1. While browsing the internet, users are confronted with persistent pop-up warnings alleging that their computer has been compromised by a virus or dangerous program.
2. These pop-ups coerce users into immediate action, often by clicking on links labeled "download" or "click here for further info."
3. Clicking on these pop-ups redirects users to deceptive websites disguised as antivirus software or tech support pages, where they are prompted to divulge sensitive information such as credit card numbers or home addresses.
4. Many users unwittingly download malware onto their devices, exacerbating their security and privacy risks.

Despite the surge in scareware incidents, users can shield themselves by remaining vigilant and adhering to cybersecurity best practices:



- Should you encounter scareware, do not comply with any demands issued by the pop-up, including clicking on links or disclosing personal information. Instead, promptly click the X in the upper right of the pop-up. Although, we might think that closing all web browsers and applications helps, it sometimes does not.

- If your device becomes unresponsive, promptly disconnect all network cables and power off the machine to contain any potential malware threats and minimize further dissemination.

- Choose “no” when asked unexpected questions. Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select “no” or “cancel,” or close the dialog box by clicking the “X” icon in the title bar.

- Be wary of free downloadable software. Many sites offer customized toolbars or other features that appeal to users. Do not download programs from unknown sites or suspicious sites. You may risk exposing your computer to spyware by downloading some of the offered programs.

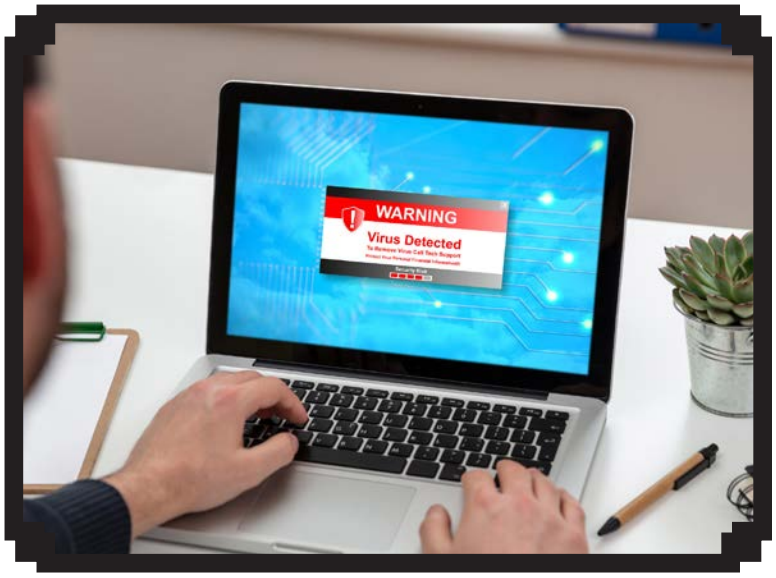
- Don’t follow email links claiming to offer anti-spyware software, like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.

- Adjust your browser preferences to limit pop-up windows and cookies. Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what web pages you have visited. You can adjust your privacy settings to only allow cookies for the web site you are visiting.

- It’s imperative to remain informed and proactive in safeguarding against scareware and other cyber threats. If you suspect scareware or any cybersecurity issue on your GFE (Government Furnished Equipment), promptly report it to the Site Manager, Area ISSO or local ISSO.

For All IHS Employees:

All IHS employees with a GFE (Government Furnished Equipment) or who use a GFE, that come across scareware or any cybersecurity incident, adhere to the following steps:



1. IMMEDIATELY contact the Site Manager or local ISSO, via email, phone or in person. Provide the date, time, location, and any other useful information. If the Site Manager or local ISSO cannot be reached, contact the Area ISSO. A contact list for Area ISSOs is located at https://home.ihs.gov/security/security-contacts/.

   The reporter, Site Manager, Area ISSO or local ISSO must initiate a computer security incident ticket by one of the following methods:

   - Email the incident details to incident@ihs.gov
   - If unable to email, call the IHS IT Service Desk at 1-888-830-7280

NOTE: It is more important to submit the report in a timely manner than it is to have fully completed it. Additional information may be provided at a later time.

2. Do not discuss any suspicious activity with others. This minimizes impact on a possible investigation.

3. Participate in incident reporting and handling as requested by the IHS Cybersecurity Incident Response Team (CSIRT) or Area ISSO.

4. If the potential incident involves an information system, perform the following actions:
   - **IMMEDIATELY STOP using the information system. Wait for further instructions from the ISSO or the IHS CSIRT.**
   - **DO lock the system (to lock your computer, press Ctrl+Alt+Delete, and then click on Lock Computer).**
   - **DO NOT turn it off, log out, or otherwise change anything.**
   - **If possible, prevent others from physically accessing the system.**

NOTE: The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites/files. Some links in this document require you to be on the IHS network or logged in to your IHS VPN. Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.