Tech support scammers are still at it: Here’s what to look out for in 2023

Hello, is it me you’re looking for? Fraudsters still want to help you ‘fix’ a computer problem you never had in the first place.

Tech support scammers have been offering bogus technical support services and “resolving” people’s non-existent problems with their devices or software for years. Using a range of tried-and-tested social engineering (https://www.welivesecurity.com/2015/12/30/5-things-need-know-social-engineering/) tricks, they’ve had considerable success duping victims into handing over their money or sensitive data such as passwords and financial details. It’s no wonder they’re still at it, using increasingly sophisticated techniques beyond phone calls and fake pop-up alerts to trick their victims.

In the US, almost 24,000 people reported losing nearly $348 million due to tech support scams in 2021, which is a 137% increase in losses from the previous year, according to the FBI. (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf) This almost certainly doesn’t capture the magnitude of the problem, however, as many victims are reluctant to come forward. Meanwhile, separate research from Microsoft (https://blogs.microsoft.com/on-the-issues/2021/07/21/tech-support-scams-adapt-2021-microsoft-study/) in 2021 claims that three-fifths of global consumers had encountered this sort of scam in the previous 12 months and “one out of six consumers were tricked into continuing with the scam”, often losing money in the process.

On the bright side, more than many others this is a cybercrime that can be prevented with a healthy dose of user awareness. By spotting the early warning signs, internet users can avoid falling victim to the schemes, saving a lot of time, money and possibly tears in the process.

How do (the latest) tech support scams work?

Tech support scams (https://www.welivesecurity.com/2018/05/07/tech-support-scams/) have evolved significantly over the past more than a decade. Early iterations involved cold calls from bogus technical support agents who were typically based in India and claimed to work for Microsoft, Dell, Cisco or another technology company, including well-known security vendors.

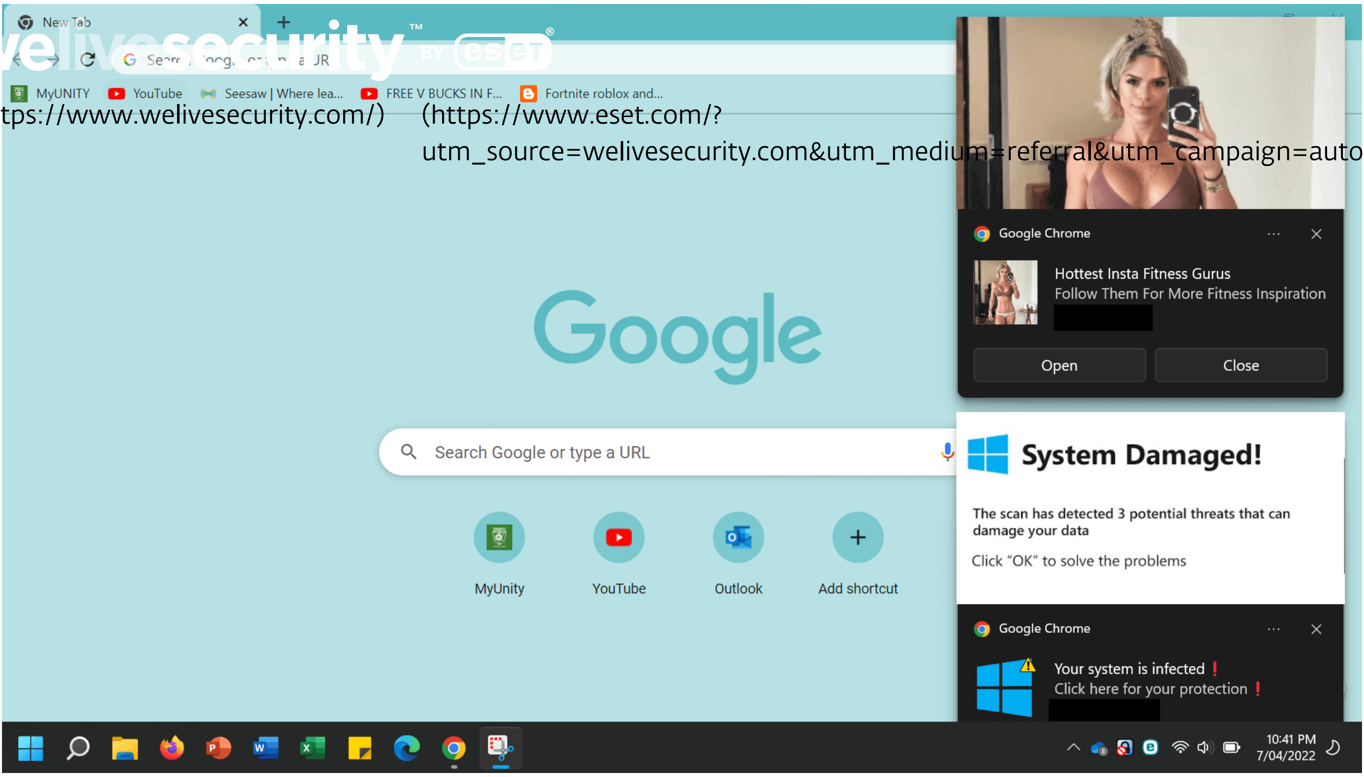
The scammers would call people out of the blue (https://www.welivesecurity.com/2017/04/10/spanish-harmada-tech-support-scams/) and in a more or less random fashion, attempting to convince them that their computer has a problem that needs to be fixed immediately in return for a fee. These attempts largely relied on finding victims with little knowledge of how computers really work and came to be supported by websites and Facebook pages offering “help” to users of specific products.

In due course, deceptive ads, bogus pop-ups (https://www.welivesecurity.com/2015/10/07/tech-support-scams-top-pop-ups/), fake support websites and attacks involving malicious and malware-like programs (https://www.welivesecurity.com/2016/02/15/support-scams-now/) emerged, with people’s computer screens showing alerts that attempt to convince them that something is wrong with their machine.

Indeed, as the scams became more diversified and sophisticated, they involved a shift where the victim is lured into calling the scammer (https://www.welivesecurity.com/2017/04/10/spanish-harmada-tech-support-scams/) (often after visiting a dodgy website), rather than scammers cold-calling people in a largely random manner.

Below are a few recent examples of such fake alerts:

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi



Google Chrome

Hottest Insta Fitness Gurus
Follow Them For More Fitness Inspiration
[redacted]

System Damaged!

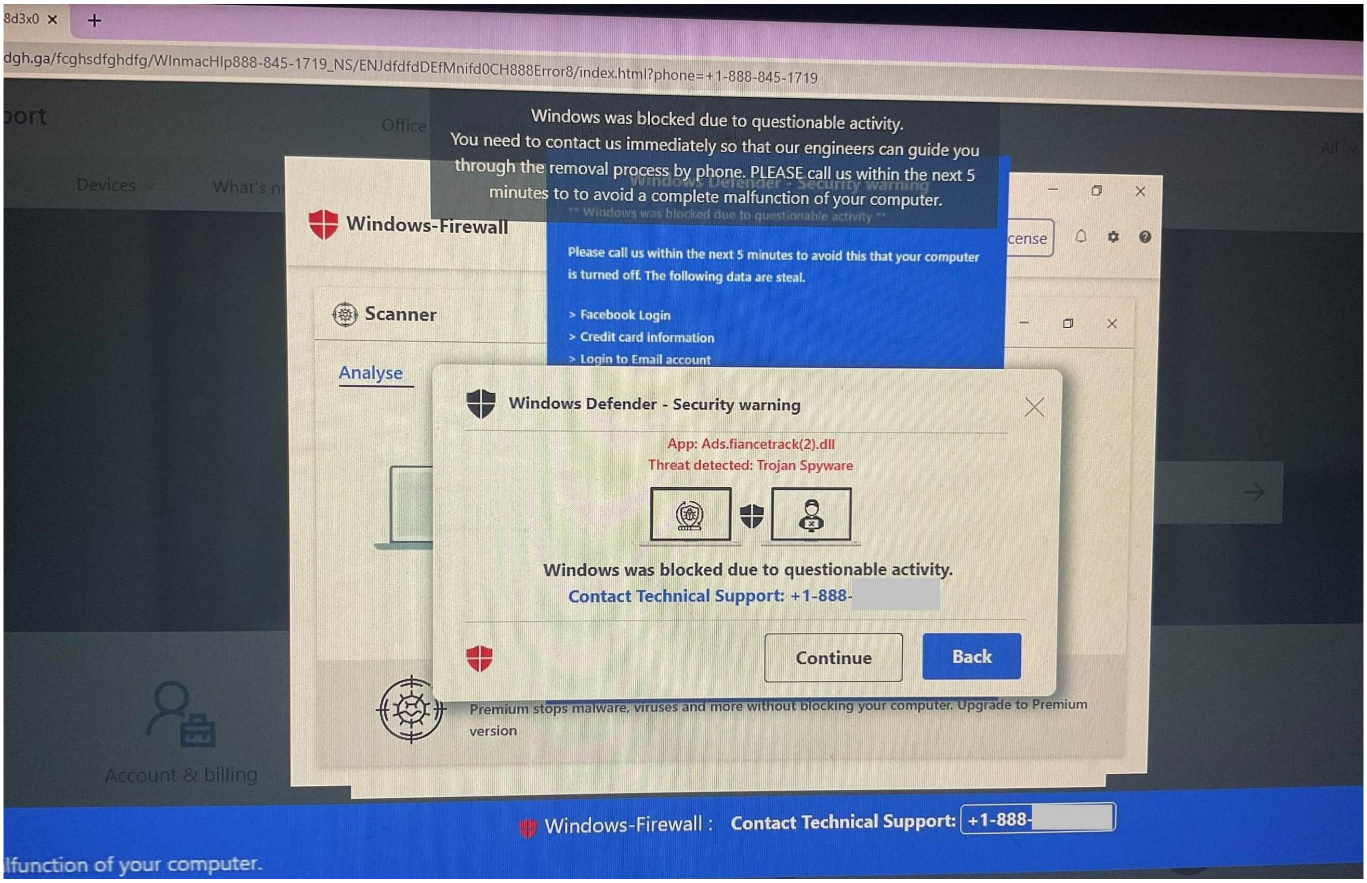
The scan has detected 3 potential threats that can damage your data

Click "OK" to solve the problems

Google Chrome

Your system is infected ❗
Click here for your protection ❗
[redacted]

(https://www.welivesecurity.com/wp-content/uploads/2023/01/tech-support-scam-example-1.png)



dgh.ga/fcghsdfghdfg/WInmacHIp888-845-1719_NS/ENJdfdfdDEfMnifd0CH888Error8/index.html?phone=+1-888-845-1719

Windows was blocked due to questionable activity.
You need to contact us immediately so that our engineers can guide you through the removal process by phone. PLEASE call us within the next 5 minutes to to avoid a complete malfunction of your computer.

Windows Defender - Security warning
** Windows was blocked due to questionable activity **

Please call us within the next 5 minutes to avoid this that your computer is turned off. The following data are steal.

> Facebook Login
> Credit card information
> Login to Email account

Windows Defender - Security warning

App: Ads.fiancetrack(2).dll
Threat detected: Trojan Spyware

Windows was blocked due to questionable activity.
Contact Technical Support: +1-888-[redacted]

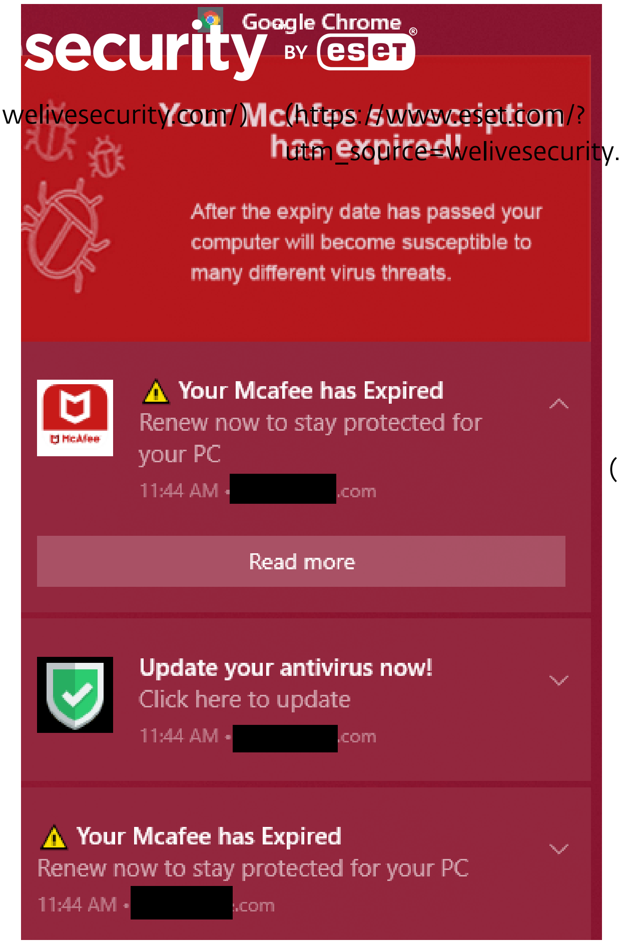
Premium stops malware, viruses and more without blocking your computer. Upgrade to Premium version

Windows-Firewall : Contact Technical Support: +1-888-[redacted]

lfunction of your computer.

(https://www.welivesecurity.com/wp-content/uploads/2023/01/tech-support-scam-example-2.jpg)

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi



Google Chrome

Your McAfee subscription has expired!

After the expiry date has passed your computer will become susceptible to many different virus threats.

⚠ Your Mcafee has Expired
Renew now to stay protected for your PC
11:44 AM • [redacted].com

Read more

Update your antivirus now!
Click here to update
11:44 AM • [redacted].com

⚠ Your Mcafee has Expired
Renew now to stay protected for your PC
11:44 AM • [redacted].com

(https://www.welivesecurity.com/wp-content/uploads/2023/01/tech-support-scam-mcafee.png)

What's the FBI's warning about?

Some of the newer tactics now also highlighted by the FBI (https://www.ic3.gov/Media/Y2022/PSA221110) involve these steps:

The victim receives an email from a legitimate-looking domain, warning of an imminent and automatic renewal of a technical service (i.e., a warranty) for several hundred dollars. The recipient is urged to contact a listed phone number or email address if they don't want to pay.

The victim calls the scammers requesting an explanation/refund.

The scammer persuades the victim to download remote desktop protocol (RDP) software (https://www.welivesecurity.com/2022/09/07/rdp-radar-up-close-view-evolving-remote-access-threats/) so that they can gain access to the user's machine, to perform technical assistance and process the refund.

The scammer will claim to have issued a refund and asks the user to log-in to their banking app to check it was successful. This will provide the threat actor with access to this account.

- Once inside the online banking account, the scammer freezes out the victim or shows them a blank screen while they secretly transfer funds out of the account.

Of course, this is not the only variation on the tech support scam doing the rounds. Another missive (https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-public-to-beware-of-tech-support-scammers-targeting-financial-accounts-using-remote-desktop-software) shared by the FBI claims scammers might cold call, text or email to make first contact with the victim. They may pretend to be representatives not just of technology firms but also financial and banking institutions, utility companies, or even virtual currency exchanges. The "problem" they are calling to resolve might not be a license or warrant renewal, but instead a compromised email or bank account, or even a computer virus.

The scammers may then:

- Convince the victim that their financial accounts have been compromised and that they need to move their funds elsewhere.
- Take remote control of the machine via the same RDP tools.
- Open virtual currency accounts to transfer over funds from the victim's bank account.

Other tactics might include:

- Secretly compromising a user's device in a "drive-by-download" that creates fake pop-ups warning that something is wrong and that they need to call a number to resolve.
- Using remote access of the victim's machine to install info-stealing malware in order to harvest card details and other personal information – and then charging the victim for the privilege.

RELATED READING: Tech support scams: 3 steps to conning unsuspecting victims (https://www.welivesecurity.com/2015/12/10/tech-support-scams-3-steps-conning-unsuspecting-victims/)

How to spot and stop a tech support scam

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi

The good news is that with a little more natural skepticism and awareness, users can avoid the shame and pain associated with being a tech support scam victim. Consider the following:

- Don’t reply direct or call the numbers posted in unsolicited emails – if in doubt, search for the company involved and call them direct to check.
- If a pop-up or error message appears on your computer screen and contains a phone number, resist the urge to call the number.
- If somebody calls you to say your computer has a problem, hang up.
- Don’t grant PC remote access to anyone you don’t personally know, including representatives calling by phone.
- Don’t give anyone your passwords.
- Don’t log in to bank or financial accounts while providing remote access on your computer.
- Be aware that scammers will always try to hurry you into making rushed decisions, often by making the victim panic. Resist the urge to do so, take a deep breath and think.
- If you’re concerned about fraudulent activity, keep a close eye on your bank account transactions.
- Use security software from a reputable vendor on all your devices.

Tech support scams have been with for more than a decade, and they’ll be around for a long time to come. We may not be sure what else to expect in 2023, but armed with this know-how, it should at least be easier to spot them.

FURTHER READING: Vishing: What is it and how do I avoid getting scammed? (https://www.welivesecurity.com/2021/06/14/vishing-what-is-it-how-avoid-getting-scammed/)

Phil Muncaster (https://www.welivesecurity.com/author/pmuncaster/)

19 Jan 2023 - 11:30AM

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center (https://www.welivesecurity.com/category/ukraine-crisis-digital-security-resource-center/)

Email... **Submit**

Newsletter

Email... **Submit**

Similar Articles

(https://www.welivesecurity.com/2023/03/29/pig-butchering-scams-anatomy-fast-growing-threat/)

Pig butchering scams: The anatomy of a fast-growing threat (https://www.welivesecurity.com/2023/03/29/pig-butchering-scams-anatomy-fast-growing-threat/)

(https://www.welivesecurity.com/2023/03/17/svb-collapse-scammers-dream-dont-get-caught-out/)

SVB's collapse is a scammer's dream: Don't get caught out (https://www.welivesecurity.com/2023/03/17/svb-collapse-scammers-dream-dont-get-caught-out/)

Discussion

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi

What do you think?

3 Responses

👍 Upvote 😝 Funny 😍 Love 😯 Surprised 😤 Angry 😥 Sad

0 Comments 1 Login ▾

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share Best Newest Oldest

welivesecurity™ BY eset®

(https://www.welivesecurity.com/)

(https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&ut

Home (/)

About Us (https://www.welivesecurity.com/about-us/)

Contact Us (https://www.welivesecurity.com/contact-us/)

Sitemap (https://www.welivesecurity.com/sitemap/)

Our Experts (https://www.welivesecurity.com/our-experts/)

Research (https://www.welivesecurity.com/research/)

How To (https://www.welivesecurity.com/category/how-to/)

Categories (https://www.welivesecurity.com/categories/)

RSS Configurator (https://www.welivesecurity.com/rss-configurator/)

ESET (https://eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotagging&utm_content=scams&utm_term=en

Privacy policy (https://www.welivesecurity.com/privacy/)

Legal information (https://www.welivesecurity.com/legal-information/)
Manage cookies

(https://www.welivesecurity.com/) (https://www.eset.com/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotaggi