Scams, Scams and more Scams

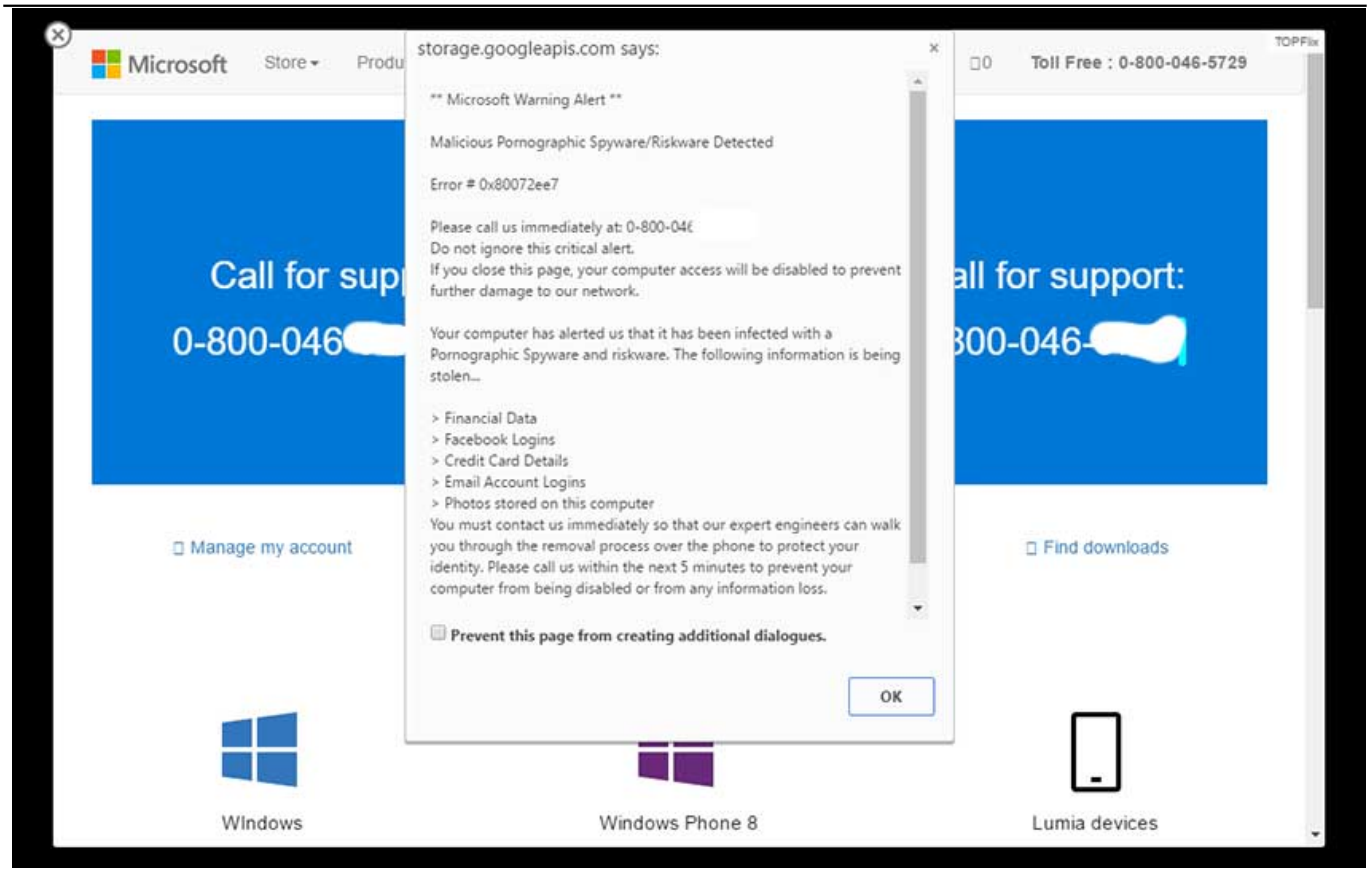
Common scams in 2018 - spot and avoid them | Tech Tips Article by PcCG

Some of the most common calls we get involve scams. Sometimes the scammers are successful; sometimes our clients call us before they get taken advantage of. We've covered them before in our tech-tips, but this will be a good refresher. We will try to be brief, but at the same time include relevant information.

1. Fake Microsoft Alerts

Fake Microsoft Warning **[1]**

Fake Microsoft Warning 2 **[2]**



You may have encountered alerts like this before. **DO NOT CALL THESE SCAMMERS OR ALLOW THEM INTO YOUR COMPUTER.** This is what we'd consider "common sense". Don't allow anyone into your computer you don't know or trust. Would you give out personal information or allow a random person showing up at your door claiming to be from Medicare? Probably not!

How can you tell it's a scam?

1. It's hard enough to get tech support from companies like Microsoft. They are not going to go out of their way to get you to call them.
2. These scammers ultimately always ask for credit card info
3. Your web browser doesn't scan your computer
4. Message often will say don't restart or turn off your computer.

What do you do?

If you know how to "end-task" on your browser, do that. If not, simply restart the computer. 75% of the time you'll be fine. It was just a webpage displaying static information. I could create a webpage saying "If you leave this page dogs will fall from the sky." That doesn't make it true; just as the warning stating restarting your computer will break things isn't true. The reason they put the "Don't restart" message is because they know it will just go away most the time and they want your credit card info.

Don't go back to the link or email that you clicked on (or URL you mistyped) again. Anytime you go to that same link/URL - you will get the same error message.

If you end up letting the scammer into your computer, and don't give them your credit card info - they may try to ACTUALLY break your computer or worse, encrypt your files.

Another thing YOU can do is to share this article (or similar educational articles) with people. The scammers are using "social engineering" to scam you. They are trying to scare you into calling them.

This isn't really an I.T. problem since they are working to manipulate you into giving them access to your computer. Knowledge is power!

All of this applies as well to random phone calls from "Tech support". Again, don't let them into your computer.

We even took the time to "go under-cover" and pretend to fall for once of these scams. We recorded the entire event - so you can hear how they work. You can find that in our Fake Tech Support Scam Video [3]

If you continue to get the message contact a trusted computer repair shop with good reviews.

2. Random Emails with your password

> I am well aware dthB1QibD one of your pass word. Lets get straight to the point. You do not know me and you are most likely thinking why you are getting this email? Not one person has compensated me to check about you.
>
> In fact, I setup a software on the adult vids (adult porn) web-site and guess what, you visited this site to have fun (you know what I mean). When you were viewing videos, your web browser started working as a Remote control Desktop with a key logger which provided me with accessibility to your screen and web cam. Immediately after that, my software program obtained your complete contacts from your Messenger, social networks, and emailaccount. And then I made a double video. First part shows the video you were watching (you've got a good taste hehe), and next part shows the recording of your cam, and it is u.
>
> You have 2 solutions. Shall we check out the possibilities in aspects:
>
> 1st choice is to dismiss this e-mail. In such a case, I am going to send your actual video to all your your personal contacts and also just consider about the embarrassment you experience. And consequently if you happen to be in a committed relationship, how it will certainly affect?
>
> Next alternative should be to compensate me $4000. We will name it as a donation. In this situation, I will instantly remove your video recording. You will keep your daily ro utine like this never took place and you would never hear back again from me.

This is the exact text from an email I received. It has the right password in there. I actually have 6 of these in my inbox right now!

Are you terrified yet? Some people are! How could they know your password if what they wrote wasn't true about a key-logger (a program that records your keystrokes)?

How can you tell it's a scam?

Remember we talked about social engineering? Here it is again! An attempt to scare you into sending money their way. But you're not going to fall for this, because you are taking the time to learn about scams!

The reason they may have your REAL password is because a website you used was hacked. We've heard about some pretty large-scale breaches lately where hackers stole information from company XYZ. That is how they obtained your password, NOT from a keylogger as the message claims. If you have an anti-virus (and everyone should), then you probably don't have a key-logger. In the database they hacked - they obtained information such as your name, email and password. They then send you this scary email full of lies. Please, don't fall for it.

What do you do?

1. Delete the email, DO NOT respond to it. *(Tempting as it may be to tell them what you really think of them, don't.)*
2. IF you still use that password anywhere - change it! *(This is why it's good to change your passwords at least yearly)*
3. Try and use different passwords for different sites. Unfortunately people use the same password for every site. Yep! Looking at you! Since they hacked one database, they can now get into ALL of your stuff! That's why you use different passwords for different sites.
4. Investigate to see if your email addresses have been compromised: https://haveibeenpwned.com/ [4]
5. Use 2FA [5] (Two Factor Authentication). Bonus points for this one! *(In Short, 2FA requires a unique code along with your password every time you log into a site. Yes it's more troublesome, but it's also extremely secure!)* (2FA Tech Tip here [5])

3. Ransomware

This one is the worst. **If your files get encrypted, you're done for.** You either have to pay the ransom and MAYBE get your files back, or not and lose them forever.

Files that are encrypted generally cannot be decrypted. One day a decryption key may become available should government(s) seize the server, but don't bank on that saving you. (Link here [6] for one possible source of confiscated decryption keys).

The key to surviving this nasty scam is to have your files backed up. Without a good, up-to-date backup (preferably automated) - you're out of luck. So do yourself a favor, and backup before it's too late [7]!

Fortunately this threat has died down quite a bit from its peak in 2017.

So there you have it! Those are the threats we see most often in 2018! I hope this is able to save you and your friends/family from the bad-guys out there on the web.

Article Tags: Tech Tips [8]
Tech Tips Articles [9]

Source URL:https://www.pccomputerguy.com/tech-tip-article-scams

Links
[1] https://www.pccomputerguy.com/file/224 [2] https://www.pccomputerguy.com/file/225 [3] https://www.pccomputerguy.com/Tech-Tips-Video-Fake-Tech-Support-Scam [4] https://haveibeenpwned.com/ [5] https://www.pccomputerguy.com/Tech-Tip-Article-2FA [6] https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor [7] https://www.pccomputerguy.com/Tech-Tips-Article-BackBlaze-Cloud-Backup [8] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [9] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles