Issue 2 Volume 9 June 2023

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Security Solutions

Helping secure your world

Editor's Note

In recent times our county has been faced with an unprecedented number of computer-generated offenses ranging from cybercrime, cyberbullying, and identity theft to name a few. Due to this; persons have adopted various methods of protecting themselves. This quarter, our newsletter will look into various methods of securing oneself when online.

If you're a Facebook user, have you ever wondered why some of your "friends" post items they ask you to copy and paste rather than share? Do you feel a little uneasy about why they asked you to do this? You should because copy-and-pasting can be used for sinister purposes. The first article discusses what this is used for and its effects. In article two, we ask the questions such as; how much do you trust your cell phone? Is it respecting your privacy or running a phone tracking app that lets others know where you are and what you're doing? And your phone knows an awful lot about you. Phone tracking software is legally available for both Android and iOS (Apple) devices in the companies' official stores. It can have a legitimate purpose and sometimes sinister purposes. See how you can spot and stop these phone tracking apps.

Keeping your personal data safe is extremely important in the cyber world, article three gives 10 tips such as two-factor authentication and using an updated browser as examples of how to keep your data safe. Keeping data safe can also help you decipher scams, however, there is always an unguarded moment because much as most of us like to think we're smart enough not to fall for a scam, millions of people are conned every year into giving access to their PCs to tech support imposters. These are the people who claim to be from Microsoft or another computer firm? They tell you they've detected a virus on your PC and need to be given remote access to put it right. The fourth article tells you what to do if you fall for this scam.

We do hope you find these articles and the safety methods helpful in some manner and we at **Amalgamated Security Services Limited** will continue to fulfill our commitment to provide quality service for all customers.

Regards
ASSL Marketing Team

Copy and Paste Plea Exposes Your Identity

If you're a Facebook user, have you ever wondered why some of your "friends" post items they ask you to copy and paste rather than share? Do you feel a little uneasy about why they asked you to do this?

Well, of course, they likely didn't ask you. They simply copied and pasted the item themselves that one of their friends previously posted -- and the request to pass it on in this way was already built in. The trail goes all the way back to the original poster. It's a sort of chain letter, which aims to reach as wide an audience as possible.

But why? Is it a scam?

Its purpose could certainly be dubious -- but not always. First, you need to understand something important about the way sharing and copy/pasting work on Facebook.

In very simply terms, when you share a post from someone who has tightly controlled privacy settings, their privacy status effectively restricts who can see it. It can't be made "public" and may not even be further shareable. But when you copy and paste an item, you're really creating a new post that can be seen by all your friends and beyond. In other words, it gets wider circulation.

So, you're being used to help amplify a message. That may or may not be a good thing depending on its content. But that's not all. By copying and pasting, you're effectively enabling the original poster to track everyone else who is repeating it.

How? The original poster inserts some text with a couple of spelling mistakes in the message. Then they do a search using the misspelt phrase. This returns a list of everyone who has copied and pasted the message.

Now, let's say the message was about gun control, animal abuse or another contentious subject.

The original poster will now have a list of people who seem to support his/her cause and they can go about trying to contact them via Facebook with "friend" requests and other messages. Their findings could also contribute to a profile of you that some marketing and research companies build. Furthermore, the original poster can delete their message and, therefore, not be easily traceable, while the copied-and-pasted versions live on.

That's not what happens with a shared message. If you delete something you shared, all the forward-shared versions of it disappear as well.

Irina Bena Blue screen on my 9 months old DELL!!!!!!!!!!!!!!!!!!!!!!!!!!!

about 15 hours ago Comment Like

8 comments

George Moga nasol! ce variantă de Win?
delete
about 15 hours ago

Irina Bena Vista.... :-(
In safe mode ruleaza inca. Ce-o mai fi anvand iar... Am mai fost de doua ori cu el la reparat. Prima data nu avea update de Bios, a doua oara se stricase ceva la ventilatie

George Moga mda, la ce te poţi aştepta de la Vista :(

Irina Bena MacBook ma tenteaza din de in ce mai mult

George Moga nici mie nu mi-ar displăcea, dacă aş câştiga unul la vreun concurs :D

Irina Bena :D

DeeDee Davy dupa un an de dell iti va ceda acumulatorul. mi s-a intamplat si mie... si unei prietene... si alteia... :-s

Irina Bena Dupa tot ce am patit deja cu el, asta mi-ar mai lipsi... cireasa de pe tort!

Add a comment

Amen To that

The same tracking tactic works for any message. You know, the type that says something like, "If you agree, comment 'Amen'." Again, by doing a search, the original poster will be able to identify all his/her supporters.

Copy-and-pasting can also be used for other sinister purposes.

For instance, if the original message is a hoax or fake news of some sort, the copy and paste version becomes much more difficult to delete because each is effectively a new original. So, as mentioned above, while deleting a shared message would remove the entire chain of forward shares (note, not earlier shares), that wouldn't happen with a copy and paste.

And, again, the original hoaxer could delete their message to keep their own identity secret, while their false message continues to circulate.

Another chain-style trick that sneaky Facebook users apply is to solicit information about you by offering to tell you something trivial about yourself, like which celebrity you most resemble, or which one would make you a perfect partner, or some other trick created to pique your curiosity. They might ask your birth date, your favorite color or even your mother's maiden name.

See where this is leading? You're giving information about yourself that potentially could be used for identity theft.

Plus, by taking part in this "game," your celebrity identity (or whatever) is entered into the post's comment field, which means the message will now most likely go to your friends. And so it goes on.

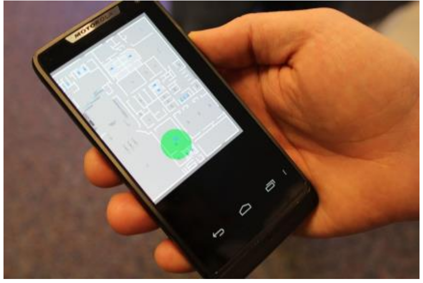
So before copying and pasting, adding "Amen" etc., or playing the celebrity game, it makes sense to pause and consider the possible implications of what you're doing -- and the information you're giving away about yourself.

The original poster's intentions may have been perfectly honorable. Or maybe they're not. And you may not find out until it's too late.

Reprinted from
Scambusters.org

How to Spot and Stop Phone Tracking Apps

How much do you trust your cell phone? Is it respecting your privacy or running a phone tracking app that lets others know where you are and what you're doing? And your phone knows an awful lot about you.



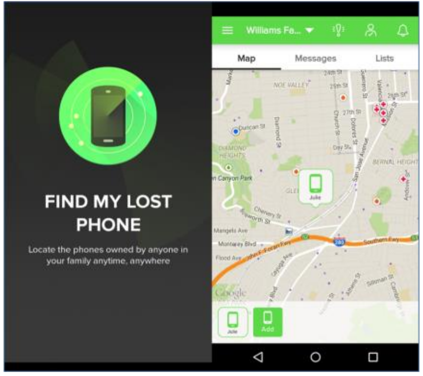
Phone tracking software is legally available for both Android and iOS (Apple) devices in the companies' official stores. It can have a legitimate purpose. For instance, it can be used by parents to keep track of their youngsters. But the same software also has less savory uses, such as spying on a partner or an employee. In some instances, it does more than just track the device; for instance, it might record phone conversations. And beyond this simple monitoring software, there's also off-store malware capable of stealing just about everything on your phone, if you let it.

As well as all these dubious activities, countless apps are legitimately capable of gathering location and even personal data -- with your permission (which they told you about in those Terms & Conditions you didn't read!). But don't panic. There's a lot you can do to spot and remove location spyware and to limit the extent to which your movements can be tracked.

Even so, it has to be admitted that the only way to guarantee your phone isn't being tracked is to switch it off -- as in powering down completely. And the only way to be 100% certain you don't have spyware is to return your device to its factory settings. Fortunately, you don't need to take such drastic actions to avoid most of the dangers.

Signs You May Have a Spy in your Phone. In most cases, spying on a phone's location requires someone to install the tracking software on the victim's phone. However, at least one tracker can work solely from a browser on the perpetrator's device. See: https://tinyurl.com/phone-track-tricks

That apart, it's not otherwise easy to install the phone tracker. The other person has to have access to the victim's phone -- either directly or via hacking and malware -- and know how to get around built-in security controls. The malicious app has to be concealed so the user doesn't spot it. But if you are one of the unfortunate ones to fall victim, or suspect you may be -- and more than one in a hundred phones are said to be compromised -- you can usually tell from increased activity on your device.


FIND MY LOST PHONE
Locate the phones owned by anyone in your family anytime, anywhere
Map
Messages
Lists
Add

You may also hear unusual background noise, like clicking and buzzing, although this is less common as tracking software has become more sophisticated. It may start to slow down or overheat, and the battery drains quickly. In some cases, it might keep rebooting itself or take ages to shut down. You might even spot an app, often with an innocent sounding name, that you don't recall installing. Or if your monthly data bill is inexplicably and sharply higher than normal, that's a powerful sign your phone is doing something you don't know about.

How to Remove Tracking Software

If you can't see the phone tracking app, you're probably not going to be able to uninstall it easily. But if you have security software on your phone, this might be able to identify it and remove it. Furthermore, some simpler tracking apps rely on your phone being continuously switched on, even when in standby mode. In this case, simply rebooting your device may actually flush out the tracker.

Some newer apps claim to be capable of detecting and removing trackers, but we haven't tested any of these so far. Otherwise, you either need to take your device to a tech expert or, as mentioned earlier, reset it to its factory state. Restoring your apps can take some time unless you have a backup that you made before the "invasion."

If you can actually identify the culprit app, you often can find specific uninstallation instructions online. How to Avoid or Control Phone Tracking

The five most obvious ways or protecting yourself from phone trackers are:

1. Protect your phone. That is, keep it out of others' hands and be wary when using it on a public Wi-Fi network. Ensure access is password protected and keep your operating system up to date.

2. Install security software. You need to do this on both Android and iOS phones, although the latter are generally more secure. In addition to traditional security programs, you can install apps that warn you when a new program has been installed. And don't click on unfamiliar links, especially on social networks.

3. Don't "root" or "jailbreak" your phone. This tactic, which enables users to install unapproved or unofficial apps, is also one of the most common ways to circumvent device security.

4. When you install a new app, take the time to read through the Terms & Conditions so you know how much information the app is going to read, store, and even transmit.

5. Know how to limit the ability of legitimate apps to track you. Learn how to switch off tracking for each individual app and for your entire phone (though you likely can't totally eliminate it without affecting programs like mapping and weather apps).Of course, your phone service provider always knows which communications tower you're using, unless, as we said before, you actually switch the device off, which seems to defeat the whole purpose of having the thing in the first place!

Reprinted from Scambusters.org

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

10 Tips for Keeping Your Personal Data Safe on Social Media

Strong passwords, two-factor authentication and good cyber hygiene will keep your personal information protected while browsing popular social media accounts.

By Susan Alexandra

Social media plays a vital role in our daily life. Websites like Facebook, Twitter, and Instagram are the most common social channels used to connect with our loved ones. With over **2.77 billion social media users** today, such social media websites make a perfect platform for identity thefts. With huge user database of private information, it is the responsibility of social media platforms to keep personal information safe.

Last week, news circulated regarding the most commonly used social media website **“Facebook” that stored “hundreds of millions” of account passwords** and left them unencrypted. All the passwords were in plain text and viewable to thousands of in-house employees. If companies like Facebook have these issues, how can we rely on other platforms?

Every year, millions of people fall victim to data breaches and identity theft. If you fall prey, it can cost you loss of personal data along with lots of stress. It happens when you let your guard down and depend so much on these platforms for your security. Online safety is the most onerous task, but few ways can help you stay safe on social media.

Here are ten ways to keep your personal information safe while still enjoying the benefits of making social media connections:

1. Use a strong password and use a password manager

People use multiple social accounts for various purposes. Nevertheless, if your password is weak, your account’s security gets compromised. Also, if you are using the same password for different accounts, all your accounts can get hacked by hackers.

Make sure to use a unique and strong password for every social account. Your password must include numbers, words, upper and lowercase letters, and special characters. The stronger password you use, harder for a hacker to crack your password. Change your password at least once a month. Try to keep different passwords for different social media accounts. If you are having a problem to manage your passwords, you can use password managers.

2. Add two-factor authentication for every social account

If you are using two-factor authentication on your social accounts, it will add an extra layer of security to them. When someone logs into your account from new location, device or browser; you will be sent a password that needs to be entered for logging into your social account. This means that every time you log in, you’ll also need to enter a unique code sent on your phone by the social media website. Many people think it's time-consuming, but if you are seriously concerned about your privacy, you need to apply two-factor authentication on your each and every social account.

3. Setup security answers and update your privacy settings

All social media platforms give you the option to limit your audience. But many people are unaware of its importance. It is necessary for every user to explore, try and overview those settings. You can also set up security questions on your accounts. Instead of setting common questions like “What is your mother's name?" or "From where you are?", use questions that are hard for everyone to think about.

4. Be careful what you share
Avoid sharing personal information online because your information, including your email address, phone number, and social security number, is worth a lot of money to hackers and data mining companies.

Take a look at your social media profiles and try to keep them barren—the people who need to know your birth date, email address and phone number already have them.

5. Use a VPN

If you want to keep your conversations, messages, and calls secure; you can use an encryption tool which is called VPN. A VPN helps you to keep your communication encrypted and secure. All your information will be passed through a secure tunnel between the websites and your VPN services provider.

If you are really concerned about your privacy, you might have a question; how do VPNs protect my data? As mentioned here "Even though all the information going to and from the customer to the VPN is encrypted, all the information being sent through the outgoing VPN server is subject to the regular rules of the wild internet."

6. Keep system up to date with antivirus

Keep your system updated with the latest antivirus. Never operate an internet-enabled computer without installing anti-malware and antivirus software. There are many paid and unpaid antivirus software available. To secure mobile devices, use antivirus apps to secure your online activity and important data.

You have a friend request.

Jane Doe (St. Louis, MO)

You have 3 friends in common.

7. Verify friend requests and block fake accounts

Platforms like Facebook and Instagram are full of fake profiles. Those fake accounts can be a hacker, a suspicious organization or even a frenemy who wants to monitor your activities.

Don't accept any friend request without verification. If someone is disturbing you, it's good to report and block such profiles.

8. Regular check your mailbox to check suspicious login attempts

Keep a habit of checking your emails regularly. Many people ignore emails from Facebook, Twitter or other social accounts. They might think that it's a notification from their friends, but it could be login attempt by a hacker, and your social platform wants to inform you about it.

If you got a suspicious email or login attempt to your account, change your password as soon as possible.

9. Use an updated browser
Use an updated browser for a pleasant browsing experience. Make sure to use the latest version of the browser that is not vulnerable to hackers. Also, don't save your passwords on your browser because if your system gets compromised, hackers can easily read your saved passwords from the browser in just a few clicks.

10. Log off to your accounts when used.

The last important and good practice is, always log off to your system when you are done with it.

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

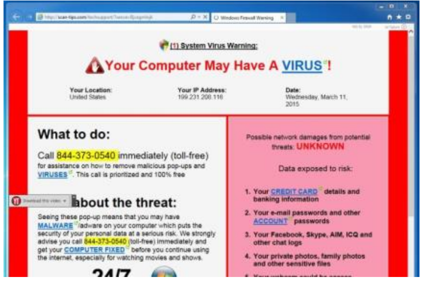
Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

WHAT TO DO IF YOU FELL FOR A TECH SUPPORT SCAM

Much as most of us like to think we're smart enough not fall for a scam, millions of people are conned every year into giving access to their PCs to tech support imposters. These are the people who claim to be from Microsoft or another computer firm. They tell you they've detected a virus on your PC and need to be given remote access to put it right. You probably know what "remote access" is, but for those who don't, it's a feature of Windows that enables someone in another location to access your PC via the Internet. But you have to give them permission via your PC first, which is why these scammers make their spoof calls. Once they get access, they can digitally crawl all over your PC, looking for confidential information like passwords and account numbers. And after they're done, they may leave a piece of malware on your PC that enables them to access it at any time or plug it into a botnet -- a network of compromised computers that are forced to send out spam.

But what if you -- or someone you know -- gets caught out and gives PC access to these crooks? According to Microsoft's Digital Crime Unit, some 3.3 million people fall victim to the tech support scam every year, costing victims around $1.5 billion. How will you know you're one of those victims? It's simple. If someone phoned you claiming to be from Tech Support or claiming they've detected a virus on your PC and they need access, it was a scam. Tech companies just don't operate that way. But tech support scammers do.

Put it this way: If they knew what was happening on your PC that would mean they must already have remote access, so why would they need to request it? So if you gave the caller access, you've exposed your PC security to them. A more clever way the scammers may try to reach you is by tricking you into downloading malware onto your PC, which then flashes a warning that you have a virus and need to contact "tech support" to have it removed.



(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location: United States

Your IP Address: 199.231.208.116

Date: Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

About the threat:

Seeing these pop-up means that you may have MALWARE /adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your COMPUTER FIXED before you continue using the internet, especially for watching movies and shows.

Possible network damages from potential threats: UNKNOWN

Data exposed to risk:

1. Your CREDIT CARD details and banking information
2. Your e-mail passwords and other ACCOUNT passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files

Again, that's not the way legitimate security software works. If it identifies a virus, it will tell you and give you the option of deleting it but genuine security software doesn't ask you to make a phone call. Once you realize what's happened, you need to take immediate action to minimize the potential damage. Or in other words, "what should I do if I gave a scammer remote access to my computer?"

HOW TO BEAT A TECH SUPPORT SCAMMER - A 10-POINT PLAN

Some of the things you should do are similar to those for identity theft. After all, that's most likely what will have happened after a scammer gets access to your computer. Here's our 10-point plan to deal with it:

1. Shut down and disconnect your device from the Internet. That puts an absolute stop on any external meddling. It also often automatically revokes remote access for when you restart.

2. Ideally, you would have a full system backup that would enable you to restore your computer to its previous state, ensuring the scammers no longer have access to your machine. If you don't know how to back up your system, you might visit the site of our friend Leo Notenboom and search on "backup." Or just do a Google search on your Internet browser - but be careful that you visit a legitimate site.

3. If you don't have a backup, run the Windows "System Restore" feature. Visit microsoft.com to learn how to do this.

4. Whether you restored your system or not, ensure your Internet security software is up to date and run a FULL virus scan to remove any lingering malware.

5. If you know how to do it, check your web browser's settings for any newly installed extensions or add-ons you don't recognize and delete them.

6. If you don't know how to do this or you're still not certain your machine is "clean," have it professionally checked. We recommend (and have used them for years, ATT Tech Support 360, a service that we trust to access our computers remotely, fix our issues and help keep us safe from tech support scams.)

7. Only when you've done all this should you change all passwords. Yes, all passwords on every account you access via your PC.

8. Alert your bank and credit card companies and monitor all statements online every day, looking for suspicious items.

9. Put a freeze on credit applications via the three credit monitoring agencies -- Equifax, Experian and TransUnion. This will cost a few dollars but is worth it. Each of the bureaus has its own "credit lock" service but you might find the following article useful: Credit Freeze and Thaw Guide.

10. File a complaint with the Federal Trade Commission (FTC).

Whether you're a victim of a tech support scam or not, make a point of educating yourself about these tricks and how to avoid them.