SLIIT
Discover Your Future

BSc (Hons) in Information Technology

Specialized in Cyber Security

Year 2, Semester 1

Adware

IE2022 – Introduction to Cyber Security

Individual Assignment

IT21184758-Liyanage P.P.

Table of Contents

Abstract

Adware is simply malware that causes damage to computers and mobile devices by presenting unwanted pop-up advertisements and finding a way to install dangerous programs. In the modern environment, there are numerous ways to introduce adware to systems, as well as numerous types of adware infections.

Adware is a security risk that is typically used to gather marketing data or display advertisements in order to generate income. This risk not only occurs much more frequently than a typical attack, but it also uses exploits that are much more potent than those found in typical malware. Without a doubt, the reason for this is that licensed organizations with experienced designers instead of amateur ones produce adware software. A rise in the prevalence of adware programs can enable data disclosure and pose a threat to system availability, privacy, confidentiality, and integrity. Businesses typically keep a ton of data that, if stolen from the wrong recipients, may cause serious harm.

Introduction to Adware

Any software program that downloads or shows an advertisement while a program is running is referred to as adware. Pop-up windows or bars that appear on the program's user interface are used to deliver the adverts. Adware is frequently developed for PCs; however, it can also be used on mobile devices. Adware that is legitimate is used to help software makers recoup their expenditures. Additionally, it can be utilized to lower or even eliminate user software costs [1]. However, occasionally the advertisements include cybersecurity risks or direct viewers to a harmful website.

Bad adware typically penetrates a user's PC while they are regularly browsing the Web. Software written by programmers can act as a Trojan horse or virus. People might, for instance, download a client for peer-to-peer file sharing that has undetected adware. After the application files are loaded onto the system, the adverts start to appear. After then, the malware might install keyloggers (programs that copy data entered via the keyboard) or trackers, or it might carry out intrusive hard drive scans [2]. A malicious adware application may communicate passwords, credit card numbers, photographs, and other sensitive information to unscrupulous individuals if it goes unnoticed, who may exploit this information to steal from the user.

How to tell if you have an adware infection.

- Slowdown computer
- Bombarded with Ads
- Constant crashing
- Browser homepage changes
- Slow Internet connection

As was already mentioned, we want to stop this adware before it damages our system and leaks confidential information. We need to comprehend how adware is implemented. Understanding adware's characteristics can help us solve this issue and stop these attacks.

Adware is a term used in cybersecurity to describe adware programs that behave dangerously or abnormally. When adware tracks consumers' online activity without their consent, it is categorized as spyware. Fraudsters take advantage of weaknesses in the ad network validation process or in a customer's browser [3].

Harmful adware can spawn pop-ups, pop-unders, and persistent windows whenever a user visits a site that has been infected. These windows allow drive-by installations. Ad blockers may put visitors at risk of infection if they are turned off. It has been discovered that specific adware programs can stop antivirus software from running. Because some adware programs are legal or lack removal procedures, security software may be unable to identify which adware programs are hazardous [3].

EXAMPLES FOR ADWARE

There are countless recognized adware applications that might have various effects on your PC. The following are a few of the most typical and/or well-known adware examples:

1. **Fireball**

   More than 250 million PCs and one-fifth of corporate networks worldwide were determined to be infected with malware, according to an Israeli software vendor. [4] Fireball is a browser hijacker created by the Chinese digital marketing firm Rafotech. Without the user's knowledge, it is installed alongside other Rafotech products, such as Mustang Browser and Deal Wi-Fi, in a bundle. It hijacks your browser when it impacts your machine. Your homepage is changed to a phony search engine (Trotux) and intrusive advertisements are added to every website you visit. And to make matters worse, you are unable to change your browser's settings [5].

2. **Appearch**

   It frequently comes packaged with other free software, and it clogs the browser with so many adverts that using it is nearly difficult. Every time you try to access a website, Appearch.info will be displayed in its place. Even if you can browse a website, Appearch will turn random text chunks into links, so every time you choose a text box, a pop-up window requesting that you download software updates will display. Along with advertisements, Appearch may occasionally display a notification informing you that access to the website you want to visit is restricted. You will then be prompted to sign up for notifications in order to access it. Even when your browser is closed, if you click "Allow," pop-up advertisements will begin to appear on your screen [6].

3. **DollarRevenue**

   DollarRevenue is intriguing despite being long since defunct because it was one of the first significant adware programs to impact millions of PCs globally. On the impacted machine, it would install a browser toolbar to keep tabs on the online searches made there. In

addition, the application would display misleading advertisements on the page and in pop-up windows. [7] It was created in 2005 in the Netherlands, and by late 2007, it had infected more than 22 million PCs globally.

4. **Gator**

Gator, a now-defunct adware application, introduced the idea of behavioral marketing to much controversy. Gator was bundled with well-known free programs like Kazaa and Go!Zilla, and it would take away website advertising and replace it with its own adverts. This meant that, if a website visitor clicked on an advertisement, Gator would receive the entire benefit rather than the content author. Gator was most infamous, though, for its practice of keeping track of users' entire surfing history and even portions of their credit card detail. They would then employ this knowledge to provide them with more precisely targeted adverts [3].

5. **DeskAd**

Another typical adware application is DeskAd, which displays pop-up adverts in addition to misleading advertisements within your web browser and traffic redirects to dubious websites. DeskAd begins extremely subtly, unlike other programs of a similar nature, and only eventually takes over your browser. Because of this, the issue frequently stays unreported until it is so severe that only an operating system reinstall may fix it [3].

DeskAd, which is typically spread via email attachments, alters the registry of the computer so that it can be launched at startup. It also duplicates itself, which can strain the processor and memory and result in a crash. The results could be disastrous if it affects a computer network.

TYPES OF ADWARE

There are two main types of adware.

1. Legitimate adware
2. Malicious adware

1. Legitimate Adware

Adware of this kind allows you to sign up for advertisements and software promotions, which enables programmers to give away their software for free by covering their costs. Users knowingly install this kind of adware in order to get anything for free. You can decide to allow it to gather marketing data as well [3]. All programmers, even reputable ones, create legal adware since offering customers a free product is an acceptable and ethical way to encourage adoption. But not every software download involves consent between the user and the provider. In this case, the distinction between legal and unlawful behavior is hazy.

2. Malicious Adware

Adware that is dishonest or abusive makes it impossible for the user to withdraw consent or solicits it through dishonest tactics. For instance, it can make it challenging to opt out of harmful third-party software or barrage the user with intrusive adverts. Adware is only deemed malicious if it is created with the purpose of providing the user with malicious software. However, some legitimate adware could accidentally produce security holes that malware can exploit.

The following are some examples of malicious adware:

1. **Spyware**

   Adware frequently contains code that monitors and logs users' online behaviors and personal information. With the user's permission, this information may be used to display advertisements that are relevant to their interests. However, if the software is used without the user's knowledge or consent, it is considered spyware. This kind of user information is frequently sold to outside parties. Computer security and privacy advocates, notably the Electronic Privacy Information Center, have expressed outrage about these intrusive activities [1].

2. **Potentially unwanted applications (PUAs)**

   Along with reputable supplemental software programs, PUAs are unwanted software bundles. They are sometimes known as PUPs, or potentially undesirable programs. Not all PUAs are malevolent, however some may engage in bothersome activities like slowing down your device or displaying pop-up advertisements. It may cause security problems like spyware and other unauthorized software and slow down a computer's performance [3].

   PUAs are typically included in open-source software and will set up while a legitimate free software installation is taking place. Since they arrive with the terms of use and privacy settings that govern the connected program, they are categorized independently of malware. Examples of potentially unwanted programs include adware, browser toolbars, browser hijackers, etc.

3. **Legal abusive adware PUA**

   lawful malicious adware PUA is made to inundate you with advertisements. Adware itself, bundled software, web browser toolbars, and other elements may contain excessive advertising. This is likewise allowed if there is no virus. Ads for stuff like fitness supplements and pornography are common in adware like this [8].

4. **Legal deceptive adware PUA**

   Legal adware that is deceiving PUA may purposefully make it difficult to refuse to install safe third-party software. Although annoying, this technique is occasionally used by legal adware [8]. If the designer did not intend to contain malware-contaminated software or advertisements, it is legal. Unfortunately, certain adware may unintentionally install malware that is disguised.

5. **Illegal malicious adware PUA**

   Malicious adware that is prohibited from usage or distribution falls under this category. The PUA makes money by sending viruses, spyware, and other types of malwares to computers. The malware might be concealed in the adware, the websites it advertises, or other software programs. This threat is intentionally being propagated by the creators and distributors, who may employ forceful methods to do so.

Today, we can see adware for different operating systems.

- **Mobile Adware**

Through popular app sectors like entertainment and gaming, adware can access people's mobile devices or cell phones. These apps could look friendly at first, but once installed, they might act maliciously.

Again, there is a range from comparatively benign to significantly more hazardous. You might download a software that, once installed, would just annoy you with adverts at the harmless end. This can be annoying, especially when the advertising occasionally shows from outside the app, making it difficult to pinpoint the source [8].

Ad clicker software and ad fraud are even more destructive. Apps that do this covertly download executable files and launch malicious processes are involved. This can involve tricking people into clicking on adverts or signing them up for expensive services that they later must pay for.

- ✓ We can utilize a browser with an ad block feature if this adware is causing the mobile device to be unresponsive. By deleting the cache memory and browsing history, these infections can also be eradicated.

- **Mac Adware**

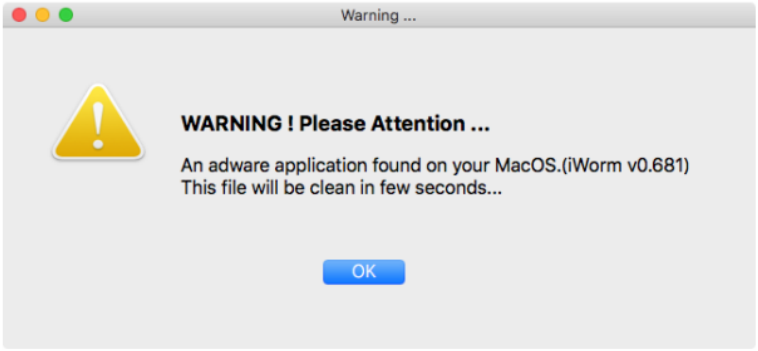
  The finest malware defense is found on Mac. The command is "xprotect." On Windows computers, cybercriminals primarily concentrate on it. Adware designed specifically for Mac computers first appeared in 2012. Since then, hackers and other groups have created the adware. Typically, a Trojan infection hides Adware for Mac inside of it.

For an example,

MacDownloader

Mac Downloader is a highly risky program. It displays pop-up messages and hides Adobe Flash Player updates. This pop-up message prompts us to enter our admin ID when we click it. Sensitive information was leaked via Macdownloader and sent to a remote site [9].

The malware will display a strange window for what is supposed to be a Flash updater: a claim to have discovered malware, if the user decides to proceed with the "update".



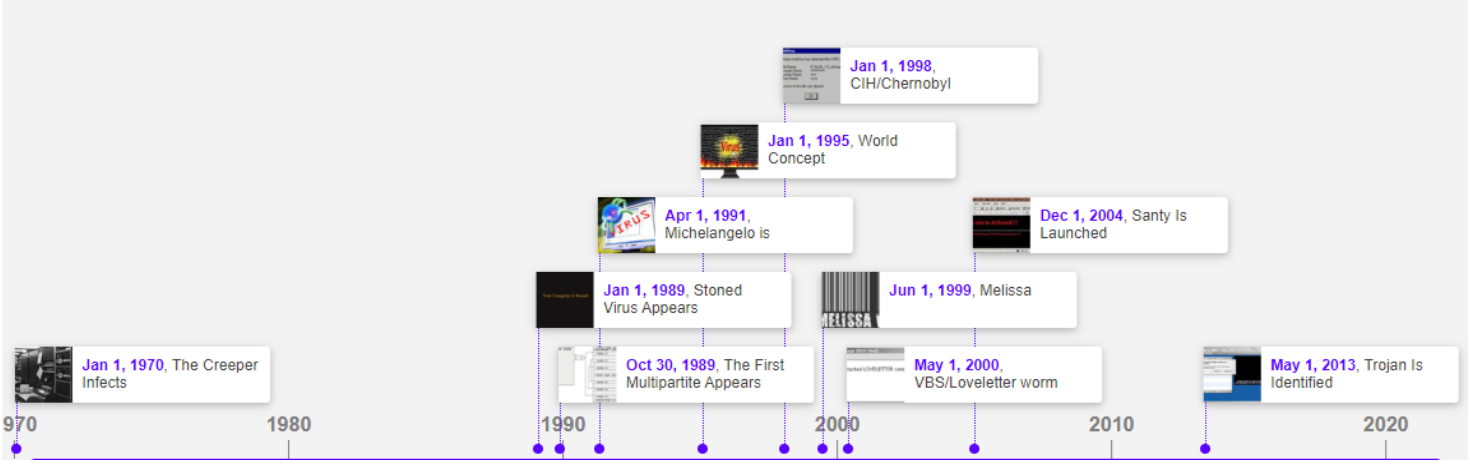
Again, the content of this notice has some phrasing and space problems, and a Flash updater shouldn't be searching your computer like anti-virus software does (It also misidentifies iWorm as "adware" when it is an old piece of malware, but the ordinary user won't notice that.). Guarnieri and Anderson, who discovered additional indications in the software that it was intended to resemble Bitdefender, believe that this malware was likely initially created as a fake anti-virus app then quickly or shoddily repurposed into the shape of a fake Flash updater.

EVOLUTION OF THE ADWARE

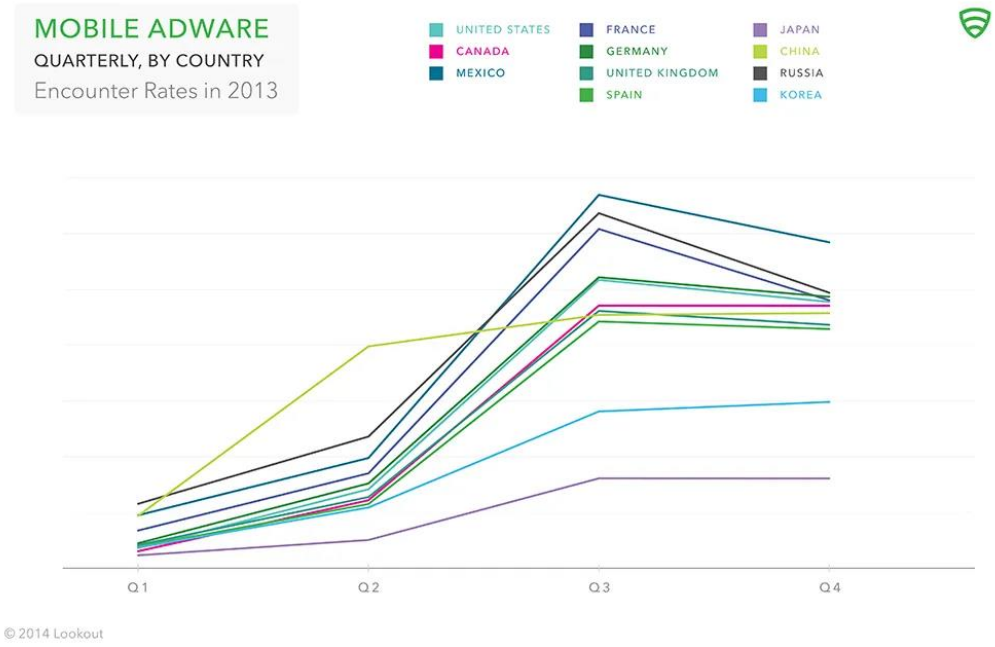
Adware was first employed online for amusement in 1987 by the Usenet newsgroup comp.sys.mac; the message refers to a Macintosh program rather than a Windows program. However, during the first 15 years after the program's implementation, until Permissioned Media, Inc. forced antivirus companies to reconsider what was and wasn't a virus, this software would not have been on the radar of security organizations. In October 2002, Permissioned Media, Inc. created a program that, like a mass-posting e-mail worm, sent a URL to itself to every person in the Microsoft Outlook contact list. The difference is that the aforesaid operation is specified in the user license agreement (EULA) during program setup [10].

Early in 2003, the free online spyware diagnostic from PC Pitstop started to find instances of spyware and offered several anti-spyware programs, including Pest Patrol and Spyware Doctor. Gator was arguably the biggest spyware provider at the time. Gator sued PC Pitstop and CompUSA after finding out that PC Pitstop had detected their product and was inebriated from ill-gotten advertising money. Gator was not classified as spyware in the complaint; rather, it was classified as adware, and damages were sought [11]. Microsoft released XP Service Pack 2 in August 2004, which fixed several security flaws in XP and Internet Explorer and did away with drive-by downloading. Gator's fortunes were reversed by Microsoft's action, and in 2008, Gator permanently shut down.

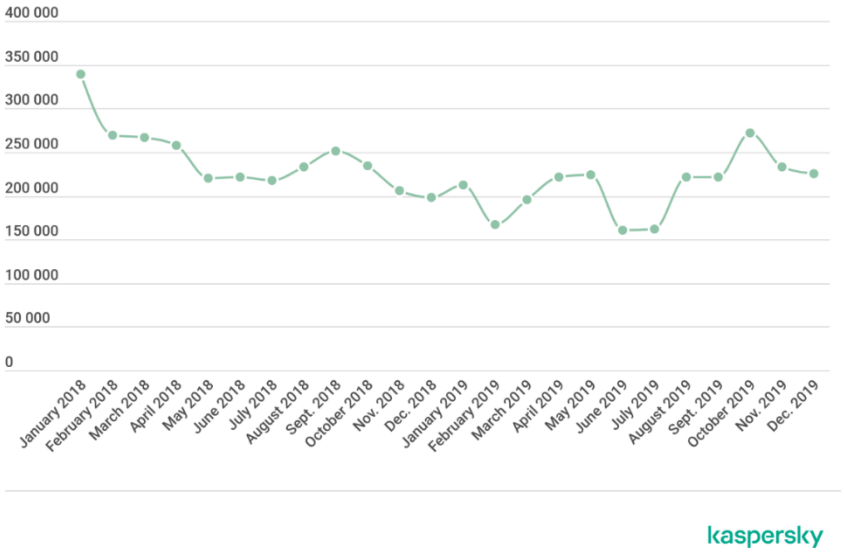
Below chart shows the History of Adware in brief [12].



In 2013, mobile adware was rapidly increased in some countries including US, Canada, France, and Russia. In exchange for their inclusion, app developers were given access to aggressive and frequently harmful advertising SDKs. Unfortunately, adware frequently took use of this deployment agreement to spread malicious agents intended to steal personal information. Adware started to decline in the third quarter of 2013, but major offenders like LeadBolt and RevMob changed their advertising SDKs in the fourth quarter, giving users a less obtrusive experience. We can see mobile adware encounter rates by the given below chart [13].



The amount of adware attacks has significantly increased in 2019, and one of their goals is to collect personal information from mobile devices. According to the data, the number of people who were subjected to adware attacks in 2019 is essentially unchanged from 2018 [14].



Today, adware is still around even if the name "spyware" is hardly used. Drive-by downloads have been discontinued. Adware now penetrates through Java and Flash player security flaws. Adware often enters through the installers of other software programs, possibly more commonly. After that, they compensate the publisher for each installation, providing them a reason to trick people into installing adware unintentionally.

Even though pop-up adverts are no longer present, adware still has the same goals in mind: to make money from our computers and our eyes. A recent adware named Conduit, which frequently uses the phrase "Trustworthy Computing," is a nice illustration. When Conduit finds gold, it installs an unwelcome toolbar and takes over all your searches in Chrome, Firefox, and IE. Even worse, it is more challenging to fully remove once it has been installed on the target system. Like 2003, almost any of the big security providers can stop and identify adware. Adware is a very bothersome web bug that is blocked by PC Matic and a few other smaller protection programs.

FUTURE DEVELOPMENTS AREA IN ADWARE

- Adware is a problematic application today, thus many firms have taken action to eliminate it. Adware creators therefore want to advance this using novel techniques.

- Future adware programs will be successful thanks to artificial intelligence and cloud-related technology.

- Adware programs currently use client internet browsing habits as a target market. Adware programs only have one area for development.

The "Phorm" cooperation

- A digital technology company is called Phorm. In Moscow, New York, and London, it is based. This occurs at a time when there is a lot of debate around the exploitation of Internet users' propensity for browsing to establish niche marketplaces with many UK IPS (internet provider service) [15].

- Horm is just one of many businesses currently in discussions with ISPs to study consumer behavior and web browsing patterns. Other names include NebuAd and Front Porch.

- Phorm's new goal comprises categorizing a user's tastes and pairing the data with the most relevant advertisements.

Online direct marketers must face three key issues: the affiliate question, user permission, and ISP judgments over what is allowed. The best protection for direct marketers is to give their subscribers something of value. That is the only defense we have. Otherwise, we will be forced to contend with a level playing field that restricts our ability to interact with consumers and decides for us what is good and wrong.

We may expect that in the future, adware will be developed more successfully using artificial intelligence. The capacity to artificially introduce human thought processes into computer programs is known as artificial intelligence. This AI concept is straightforward. This could raise the danger of adware.

Nowadays, we are mostly using Cloud storage to save our personal and important data to decrease impact of other Malware and Viruses. Cloud storage may also be negatively impacted if adware infects cloud computing. Adware has the potential to leak data into cloud storage since it occasionally behaves like spyware. This may also be seen as a significant advance in adware. If you've ever worried about adware, you might want to pay close attention and find out how it affects you soon.

HOW DO YOU DETECT ADWARE?

The following are some signs that a desktop or mobile device is infected with malicious adware [3]:

Computer adware infection signs

- a sudden modification to the home page of your web browser
- Your visited websites are not displaying properly
- having a pop-up ad overload, sometimes even when not using the internet
- Performance issues with devices
- device failure
- slow internet speeds
- Internet search redirects
- appearance at random of a new toolbar or browser extension
- You are taken to a different page each time you try to access a site.

Mobile adware infection signs

- Your phone is clunky.
- Apps load more slowly.
- Your battery quickly reduces.
- You downloaded apps to your phone that you can't remember.
- Unaccounted-for data usage and higher-than-expected phone costs are also present.
- There are several pop-up ads.

HOW TO REMOVE ADWARE?

There isn't a one-size-fits-all method to get rid of adware from your computer. It may only take deleting a browser extension and restarting your browser to get rid of some types of adware. To successfully detect and remove some additional types of adware, you might need to use adware removal programs. Even the greatest antivirus software may not be able to completely remove some types of adware. Reinstalling your operating system can be the last option in those uncommon circumstances [14].

You can attempt removing it in a few easy steps if you think your computer has an adware infection.

Step 1: Create a backup of the data

A data backup is when you copy your important system and personal data to a hard drive or external device, like a USB drive. Because they safeguard your information in the event of a system failure or data corruption that results in data loss, backups are a crucial component of computer maintenance [3].

Everyone, including people and corporations, dread losing important information permanently if no one backs up their files. Create a copy of your files and store it somewhere other than the main device. This is always a suggested initial action when managing a possible infection. Use an external device or upload the data that is most important to you to the cloud.

Step 2. Download your security software

To clean your device, we will need to install or run updates for a scanner like Adwcleaner, Malwarebytes, etc. that specializes in getting rid of adware and potentially unwanted apps. If you don't have access to these tools but suspect your computer may be infected, you can download them on another computer and transfer the security software to yours via a physical storage device.

Step 3. Remove apps that are no longer in use.

Installed apps consume important disk space and affect performance, particularly if they include components or processes that are set to run in the background. Like adware, this can happen continuously or as soon as you switch on your laptop.

It is possible to free up disk space and other resources like CPU and storage by uninstalling apps you do not use or don't need. Before removing the adware with a security program, make sure the package has an uninstaller [3]. Users of Windows PCs can access the add/remove apps list by opening the Windows Control Panel. If there is an unwanted program, select the Uninstall tab. Even if you are not prompted to do it following the removal of the adware then restart device**.**

Step 4: Perform a scan using an application to remove PUAs and adware.

Adware will likely be separated after the tool has searched for it and found it so that the user may choose to analyze it and decide whether to remove it. It is best to totally remove the PUA from your computer, rather than quarantine it or disable its features. Adware will be eliminated along with any other lingering files that can lead to its reintroduction [3].

By recognizing the name of the adware program and removing it using the device's application maintenance utility, users can manually uninstall adware from a device. This requires that the user be aware of the adware's name, which can be challenging to determine. Additionally, even after being deleted, adware that possesses a resuscitator can reinstall itself immediately.

Adware can be eliminated with cybersecurity tools as well. Adware, spyware, and other malicious programs can typically be found and removed using most endpoint security suites. There are several free software tools available to assist computer users in locating and removing unwanted programs, such as Adware's Ad Block. There are also pay-per-use programs, like the Adware Removal Tool from Bitdefender.

HOW TO PREVENT ADWARE?

Adware can make browsing difficult and slow on your device. However, it is essential to keep calm and carry out the adware removal process as described in the previous section. To completely prevent adware out of your systems, you can also stick to best practices.

1. **Exercise caution with your general digital hygiene**

   Being protected from online threats is more important than ever in today's always-connected society where media is broadcast, and programs are housed online. In the same way that good physical hygiene helps prevent physical infections, good digital hygiene can help safeguard your data and endpoint systems online [14].

   Protecting your device from viruses and other malicious applications is part of good digital hygiene. For digital equipment to operate at its best, it also needs routine maintenance. The following practices are advised: changing passwords frequently, actively limiting one's social and digital footprints, clearing one's inbox, getting software only from trusted sources, and keeping backups. Some support the use of technologies like firewalls, access control lists, and two-factor authentication.

2. **Constantly keep your operating systems (OS) and software updated**

   Malicious adware and malware infections can affect any software or OS. To address any emerging known vulnerabilities, software vendors frequently offer updates and upgrades. As a normal procedure, evaluate and apply all recent software changes [3]. This contains:

   - Regularly updating your operating system, software programs, browsers, and plug-ins
   - routine maintenance to ensure that all software is updated
   - examining log reports to look for adware signs

3. **When using the internet, adopt a "zero-trust" mentality**

An individual should consider anything strange or new in the digital world as a potential threat, according to a zero-trust perspective. Hackers employ a variety of techniques, such as USB charging ports and social contact impersonation, to install malware and adware on computers. Users should always proceed cautiously and question themselves, "What is the worst that may happen if this is malicious?"

In order to prevent installing adware on a computer, it is also imperative to be cautious of any websites that seem dubious [3]. You should use caution when downloading freeware and shareware, and only do so from reliable sources that you are familiar with and trust. If users are unsure whether a website is secure, they can read online reviews. Look for user comments and a summary of the shortcomings in reviews that are constantly available for everything from web applications to computer software.

4. **Keep an eye out for the details**

Be mindful of everything you view, download, and execute on your computer, whether it's a legitimate application download or a URL in an email. Fraudsters try to mimic reliable URLs, addresses, and social media profiles. If you pay great attention to these, you will notice odd components that are fraud red flags.

This also implies that you should carefully examine the terms and conditions of the software [1]. During program installation, be sure you have read all the terms and agreements before clicking "next." The majority of promoted third-party programs have opt-out nature, thus you should uncheck a box to prevent any associated PUA from being installed.

5. **Avoid freebies that are being promised**

In addition to the obvious risks, downloading movies and software online could put you at risk of dishonest criminals who take advantage of people's demand for "free" things. Such services may promote the installation of adware or deliver damaged downloads, whether customers are aware of this. Use only trusted, reliable sites to download software whether using the internet, downloading PC software, or using mobile applications [14].

You should try to limit your installation to reliable websites and brands whose names you are familiar with. Like reputable official application marketplaces like Google Play, they have a solid track record. Although they occasionally contain malicious software, these take precautions to protect consumers.

6. **Be aware of high costs and media manipulation**

Some advertisements manipulate media in order to profit from unintended clicks. This refers to fake close buttons, accept function keys that are positioned purposefully, and unexpected pop-ups that are all designed to entice users to click on a harmful link. Avoid clicking on buttons with excessively prominent or "in your face" design. Additionally, keep a watch on your bank statements because ominous subscription charges could mean that you have mobile adware on your device [3].

As a summery, we can follow these guidelines.

- ✓ Be careful when download any software
- ✓ Be aware of freeware and pirated apps
- ✓ Read license agreements carefully before installing any software or app
- ✓ Use a pop-up add blocker for the browser
- ✓ Do not click any adds if they are not being trusted
- ✓ Install anti-virus software

Conclusion

Recently, using adware on the internet to generate cash has grown in popularity among vendors. One obvious explanation for this is because modern tools are more mature and individuals are more connected than ever before, which increases the risk to user privacy, system integrity, and informational secrecy. A specific hazard is created by people who can freely install applications such as software, games, and other things. It has been confirmed that most people don't read license agreements, which results in Internet sites, online commercial services, and other applications over which users have no knowledge or control.

Prior to implementation, the increased risk of individual computer compromise on the internet should be considered while assessing the threat of E-trade resolutions. Together with appropriate person awareness and education supported by corresponding corporate protection measures, the conventional protection strategy of "defense in depth," such as computer terminal restrictions, can help to limit the risk from adware.

Finally, you may lower the risk of adware on your computer or mobile device by installing a reliable antivirus program. Additionally, it is wise to prepare for all the cyberattacks that the future world may bring.

References

[1] B. Lutkevich, "TechTarget," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/adware. [Accessed 20 10 2022].

[2] G. Starr, "techwalla," [Online]. Available: https://www.techwalla.com/articles/how-does-adware-work. [Accessed 20 10 2022].

[3] C. BasuMallick, "spiceworks," [Online]. Available: https://www.spiceworks.com/it-security/security-general/articles/what-is-adware/. [Accessed 20 10 2022].

[4] checkpoint, "checkpoint," [Online]. Available: https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/.

[5] Wikipedia, "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Fireball_(software). [Accessed 20 10 2022].

[6] T. Moes, "SoftwareLab," SoftwareLab, [Online]. Available: https://softwarelab.org/what-is-adware/. [Accessed 20 10 2022].

[7] wikipedia, "wikipedia," wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/DollarRevenue. [Accessed 21 10 2022].

[8] kaspersky, "kaspersky," [Online]. Available: https://www.kaspersky.com/resource-center/threats/adware. [Accessed 22 10 2022].

[9] malwarebytes, "malwarebytes," malwarebytes, [Online]. Available: https://www.malwarebytes.com/blog/news/2017/02/macdownloader-malware-targeting-defense-industry. [Accessed 22 10 2022].

[10] C. E., "Techniques of adware and spyware," in *Fifteenth Virus Bulletin* , Dublin Ireland, 2005.

[11] chengrob, "pcmatic," pcmatic, 1 11 2013. [Online]. Available: https://www.pcmatic.com/blog/history-adware/. [Accessed 23 10 2022].

[12] MrOnlyThis, "History of Adware," [Online]. Available: https://www.timetoast.com/timelines/history-of-adware. [Accessed 23 10 2022].

[13] P. Paganini, "securityaffairs," 22 2 2014. [Online]. Available: https://securityaffairs.co/wordpress/22425/cyber-crime/malware-mobile-devices-security.html. [Accessed 24 10 2022].

[14] Kaspersky, "securelist," Kaspersky, 25 2 2020. [Online]. Available: https://securelist.com/mobile-malware-evolution-2019/96280/. [Accessed 24 10 2022].

[15] wikipedia, "Phorm," wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Phorm. [Accessed 24 10 2022].