MySurvivalAlliance

8 SIMPLE STEPS TO PROTECT YOUR FACEBOOK ACCOUNT

1. Remove your birth date from your Facebook profile.

2. Stop and check your Facebook privacy settings

.. Continue Inside

HOW TO PROTECT YOUR PRIVACY ONLINE: THINGS TO REMEMBER

With the recent advances made in the field of information technology, a lot of human activities are now being done in the virtual world or online, as most netizens would describe it.

This drastic shift to the internet platform may have provided certain benefits but it has also posed some threats, particularly, to the personal privacy of these internet users, including you. Be that as it may, this does not imply that you should quit using the internet and return to your primitive way of life.

There are ways that you can resort to on how to protect your privacy online and ensure that you have a worry free internet experience.

Here are a few practical suggestions which have been proven by time and use on how to protect your privacy online. Please remember that these suggestions will not absolutely shield you from any untoward incidents while you are surfing the net, rather, they are intended to limit your exposure to risks while you are online.

1. Use an internet browser which has been proven for its security features. Having said this, one of the ways on how to protect your privacy online is to refrain from using Internet Explorer as your web browser.

   You have to remember that millions of users depend on the Internet Explorer for their surfing needs. With this number of users, the risk that more people will steal your personal information is relatively great. By using other internet browsers, you effectively distribute the risk of personal information theft.

2. If you can help it, do not always use Google when surfing the net. Take note that Google generally keeps track of all your activities while you are on the net. The more that you use Google, the greater is the possibility that your privacy might be invaded.

3. Mask your identity by using an anonymizer. You have to take note that each time you surf the net, you are basically leaving a trail through your IP Address. When it comes to the internet, your IP Address can basically disclose your identity, even some personal details which you do not want the general public to know. To the extent possible, you should hide your IP address by making use of an anonymizer. This is one good way how to protect your privacy online.

4. Never give out personal information such as credit card numbers, personal details like date of birth and the like. If you want to protect your privacy and avoid the inconvenience of an online privacy intrusion, you have to make sure that no one, other than the people you trust gets hold of your vital personal details.

With these practical recommendations on how to protect your privacy online, if you follow them, you can be assured that the risks that are associated with using the internet can be controlled and minimized to a certain extent. You have to be careful though because even with these tips, there are certain people who are just waiting to take advantage of your vulnerability online. As they would say, prevention is always better than cure. So, be safe while you are online.

ARE CRIMINALS SPYING ON YOU WITH YOUR OWN WEBCAM?

IT'S POSSIBLE.

Webcams are everywhere. They're on buildings giving feeds on traffic, crowds, and activity. They're in homes for personal use and businesses for web conferences and presentations. For something most people have used at one time or another they can seem like toys that you have complete control over.

But what if someone could access those personal cameras without your knowledge to spy on every little thing that's going on and you do? Access to things online that most people consider private are finding their ways to the public domain without their knowledge. As today's criminals become more and more tech---savvy, the possibility of your webcam falling prey to them is increasing on a daily basis.

One new website (which has since been taken down) allowed you, your neighbor, your ex, your nemesis---anyone---to view unsecured webcams at will. While this instance is limited to one particular brand of webcam, a reader would only need to browse the comments for the article at the Gizmodo link listed at the bottom of this article to see that this is far from being an isolated glitch.

Webcams, like anything running an operating system connected to the Internet (your smartphone, laptop, house alarm), require regular updates such as software patches... like when your computer seems to annoyingly always ask you to update the system, often referencing security vulnerabilities that need patching. Although the compromised webcams seem to be limited to individual homes and certain office spaces, it's little loopholes like this that enable a thief or terrorist to establish employee patterns, learn access codes or identify possible weaknesses. If it's online, it has the potential to be seen by just about anyone if you are not careful.

Technology isn't perfect. It can fail and does. But often times user error forces its demise due to lack of proper maintenanc. That's why it's important to stay alert and make sure all needed updates are downloaded and precautions are taken. Updates give technology the ability to adapt as thieves are always looking for ways to compromise the technology to their benefit. Don't let criminals use your own tools against you.

Protect your business or home by occasionally checking yourwebcam provider's website or making a quick call to see if there are any notifications. Webcam companies will usually offer free updates to their products that will make things hum along while keeping the devices and secure from prowling thugs.

SIGNS THAT SOMEONE IS SECRETLY SPYING ON YOUR EMAIL ACCOUNT

Do you suspect that someone has stolen your passwords and is secretly reading all your private emails? Chances are that if you have this gut feeling your feeling is correct. These days it's fairly simple to steal a person's password and you don't have to be some kind of computer genius or elite hacker to accomplish this.

If you do a simple Internet search you'll find that it's very simple and inexpensive to purchase a key logger. A key logger can either be a software secretly installed on your computer or a small piece of hardware attached to your system. Either method will record every keystroke typed on your computer even the passwords you enter when logging on to your email accounts. The key logger will record this info and then secretly email the data to your hacker.

You'll also find an abundance of trojan and phishing tools to trick a person into giving away their secret email passwords. These are types of spyware or computer virus that you may receive via email or an email attachment. Once these programs are downloaded to your computer they will record your passwords and email that information to the hacker.

The Signs of a Hacked Email Account:

1. Sent emails you never sent.
2. Deleted emails you never deleted.
3. Read emails you never read
4. People know your secrets
5. People show up at places mentioned in emails

If you have noticed any of these signs it is very likely that someone has invaded your privacy and is reading your emails. Many people will suggest that you immediately change your passwords and notify your email provider. But if you want to catch your hacker in the act it's best to consult with a private investigator that has the tools and experience to catch your hacker and document the crimes and take that report to the police.

A private investigator can remotely monitor your email account and document and third part access to the account. He can tell if anyone other than you is accessing your email account. He can take that information and use it tolocate and identify the hacker. In many cases a follow up investigation involving a forensic hard drive examination can recover enough evidence to identify the hacker and get an arrest and conviction. If you have a suspicion you're probably on to something. There is help available and you can restore your safety and security.

FACEBOOK PRIVACY TIPS: 8 SIMPLE STEPS TO PROTECT YOUR FACEBOOK ACCOUNT

8 simple steps to protect your Facebook profile and the information you feed into it. Learn more about the security and privacy policy within the social media site so you can control information, protect yourself from internet predators and have fun using a valuable communication tool.

Remove your birth date from your Facebook profile.

Stop identity theft by removing this simple piece of information from your Facebook profile. Remember the last time you lost your password and you called your bank, credit union or insurance? They probably asked for your name and date of birth.

By displaying your full birth date you potentially giving access to your password resets from your bank and credit accounts. Go to your profile page and click on "Edit profile" (Under your Profile picture). Under the Birth date tab, change to "Show only month and Day in my Profile" or "Don't show my birthday in my profile". It's amazing how much you can find out when you use a person's name and birth date!

Stop and check your Facebook privacy settings.

Stop giving access to all users to view your profile. From your privacy menu which can be found Account > Privacy Settings, limit access to people you don't really know. As a basis you should only allow access to your friends; however on new accounts Facebook will default to "Everyone" for all privacy settings. You can restrict access to your personal information, photos, friends, religion, contact and family information. You can even create custom friend groups to limit access to information.

Phone numbers and address should only be trusted with immediate family and friends who you regularly stay in contact with. Remember: Use "Customise" for custom privacy settings and if you select "Friends of friends" then the information can be viewed by all your friends along with everyone on their friends list.

Stop tagging photos of children

Stop tagging your children in photos. Don't use your children's name in photo tagging. If you see someone who has tagged your child's name, then click on the "Remove tag" button underneath the photo. If your child name was manually typed for the tagging, then contact the owner to get the name removed. Protect your childrens privacy from the predators who prowl the net by removing their names from photos. It is also a good idea to remove the date and time fields which may have printed on the photo.

Stop young children from using Facebook.

You must be at least 13 years old to use Facebook (From Facebook Privacy Policy) and own a profile. If you have a young child or teenager who uses Facebook, monitor their activities by either providing your email for notifications or using third party software to control internet usage. Educating children in using the internet and how information can be spread to millions of users is an important aspect for all parents. Teach children about posting status updates regarding dates, times and even school information.

Stop updating your status with "Away from home Messages"

Stop mentioning you will be away on holidays or extended leave. Do you personally know every single person on your friends list? I'm guessing it's "No". By stating on your status or providing dates when you will be away from home or the office is inviting people to snoop around your premises.

Search Google for robberies and holdups while users twittered and updated their status to "Away from home". Recently law enforcement advised Facebook users to rethink what they place into their status fields for Facebook and Twitter. A tip: consider updating your friends after you return from holidays and try to keep dates and times to a minimum.

To disable this feature, go to Account > Privacy Settings > Search > “Public Search results” > Remove tick in box. After disabling this function, Google will remove your listing within 1 ---5 weeks. Exact time frame for search engine removal currently unknown.

Stop and check Facebook Application Settings

Stop using Facebook applications with share information to third party sites. FarmVille and Mafia Wars are not the only apps found on Facebook. There are millions of Facebook applications which can be download and used on Facebook and on your web site. Protect yourself from these applications and your friends applications by visiting Account > Privacy Settings > Application and Web Sites.

From here you can control what friends share about you on Facebook. It also controls what applications can use from your profile when you install on your profile or web site. Instant Personalization Pilot Program is when web site chosen by Facebook can customise their web site with the information from your profile. Untick to remove this feature.

Stop and change your Facebook Password

Stop using weak passwords or words which can be found in a dictionary. This is the most common hack known on the internet when users use dictionary attacks on usernames and passwords. Always ensure your password is at least 8 characters and you have both number and letters combined. Always update your passwords at least every 3 months. If you want free software to help remember your passwords, fill forms and auto logon consider these free applications. KeyPass and RoboForm.