Is Facebook a secure platform to communicate with your friends and family?

Facebook is one of the most popular sites in the world, with ***everybody***. It is not as inherently secure as people think it is when they log on every day. And the vulnerability is not limited to expert computer hackers. It takes no training at all for anyone to harvest information from what you willingly offer to the public.

The potential for crime is real. The Internet Crime Complaint Center, also known as IC3, is a multi-agency task force started by the Federal Bureau of Investigation (FBI). In 2012, the IC3 received reports totaling over half a billion dollars in damages to consumers. If you're not carefully using Facebook, you are looking at the potential for identity theft or physical harm to you or your loved ones if you share information. One police agency recently reported the number of crimes they've responded to in the last year involving Facebook climbed 346 percent. These are real threats.

Lately, it seems a week doesn't go by without some new news about a Facebook-related security problem. The site is constantly under attack from hackers trying to spam the 1.23 billion Facebook users, harvest their data, or run other scams.

The danger is not just economical. Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass. Cyber stalking is often accompanied by real-time or offline stalking. A stalker may be an online stranger or a person whom the target knows. He or she may be anonymous and solicit involvement of other people online who do not even know the target.

Do people really have privacy on Facebook?

No. There are all kinds of ways third parties can access information about you. For instance, you may not realize that, when you are playing the popular games on Facebook, or take those popular quizzes, every time you do that, you authorize an application to be downloaded to your profile that you may not realize gives information to third parties.

Does Facebook share info about users with third parties?

Absolutely, and they are trying to get you to share as much information as possible so they can monetize it by sharing it with advertisers. Facebook shares the information in your profile with all kinds of third parties, so they can have a better idea of your interests and what you are discussing, so they can - as they portray it - "make it a more personal experience."

Is it in Facebook's best interest to get you to share as much info as possible?

Again, absolutely. Facebook's mission is to get you to share as much information as it can so they can share it with advertisers. The more info you share the more they are going to with advertisers and make more money.

But I can deactivate my account?

Few users know this but Facebook doesn't erase your data when you deactivate your account. This means that even after you quit Facebook, the company can still use or sell your information to 3rd party advertisers, etc.

Isn't there a security problem every time they redesign the site?

Every time Facebook redesigns the site, which happens at least a few times a year, it puts your privacy settings back to a default in which, essentially, all of your information is made public. It is up to you, the

user, to check the privacy settings and decide what you want to share and what you don't want to share. Facebook does not notify you of the changes, and your privacy settings are set back to a public default. Many times, you may find out through friends. Facebook is not alerting you to these changes; it is just letting you know the site has been redesigned.

Can your real friends on Facebook also make you vulnerable?

Yes again. Your security is only as good as your friend's security. If someone in your network of friends has a weak password and his or her profile is hacked, he or she can now send you malware.

A lot of websites we use display banner ads, but do we have to be wary of them on Facebook?

Absolutely: Facebook has not been able to screen all of its ads. It hasn't done a great job of vetting which ads are safe and which are not. As a result, you may get an ad in your profile when you are browsing around one day that has malicious code in it.

Is too big a network of friends dangerous?

You know people with a lot of friends, 500, 1000 friends on Facebook? What is the likelihood they are all real? There was study that concluded that 40 percent of all Facebook profiles are fake. They have been set up by bots or impostors. If you have 500 friends, it is likely there is a percentage of people you don't really know and you are sharing a lot of information with them, such as when you are on vacation, your children's pictures, their names. Is this information you really want to put out there to people you don't even know?

Stalkers love Facebook.

Let's face it; the Facebook Timeline is like a scrapbook for stalkers. Timeline provides an easy interface where your friends, and depending on your privacy settings, any one in the world can have quick access to all the things that you've ever posted on Facebook. Stalkers just need to click on the year and month that they're interested in and Facebook

Timeline takes them right to it. Nearly every aspect of your life is potentially on display for stalkers to follow. From the music you're listening to, to where you're "checking in" at in the real world, these little tidbits of information can help your stalker learn your patterns so they can know where to find you. It's best to limit the sharing of your location on Facebook as much as possible or not share it at all. Use Facebook friends' lists to organize your friends. Create a list of your most trusted friends and set your privacy settings to allow more access for trusted friends and highly limited access to acquaintances that might end up being stalkers.

Thieves love Facebook.

Want to make yourself an easy target for thieves? The easiest way to do this is to share your location information on Facebook. If you just "checked-in" at the local gym and posted this to Facebook, then any thief who is trolling Facebook profiles will know that you are not at home. This would be a great time to rob you. You may have restricted your privacy settings on Facebook to just friends, but what if a friend is logged into a publicly accessible computer, such as at a library, and forgets to log out or has their cell phone stolen? You can't expect that your friends are the only ones who have access to your status and location just because your privacy settings are set to friends only. Some Facebook apps that share your location may have more relaxed privacy settings than you are comfortable with and may be blabbing your location without you realizing it. Check your privacy settings and also check to see what information your Facebook apps are sharing with your friends and the rest of the world. Limit them as much as possible to protect your privacy and personal safety. Never ever post that you are home alone.

Lawyers love Facebook.

Anything you do on Facebook can and may be used against you in a court of law. Lawyers absolutely love Facebook because it helps greatly in establishing a person's character and where and when something took place. Facebook does a lot of legwork that a private investigator

would normally have to do, such as learning who a person associates with (i.e. who their friends are). Are you in the middle of a custody battle? Posting pictures on Facebook of yourself getting tanked at a party could help your ex-spouse with their case against you. Facebook postings often reflect our moods. A ranting status post might get you labeled aggressive or abusive by a lawyer trying to make a case against you. Avoid posting while you're angry or drunk. If you're tagged in a picture that might be considered inappropriate, you can "untag" yourself so that the picture is not associated with your profile. Remember that even if you removed a posting after it appeared, the post might have still been caught in a screenshot or sent in an email notification. There are no guaranteed take-backs on Facebook, so always think before you post.

Employers watch your Facebook activity.

Whether you're at work or not, your actions can affect your company's image, especially since most people put who they work for in their Facebook profile. If your employer reviews Facebook activity and sees a ton of it while you're supposed to be working, they might use this against you at some point. If you say you're sick and then your Facebook location says your checking-in at the local movie theater, this might tip off your employer that you're playing hooky. Potential employers might also request a look at your Facebook profile to learn more about you. You might consider reviewing your Timeline to see if there is anything that might cause them not to hire you. Worried about your friends posting something stupid on your wall or tagging you in an unflattering picture that might affect a potential job offer? Turn on the Tag Review and Post Review features so that you can decide what gets posted about you before a post goes live.

What you should never put on Facebook

1. You or Your Family's Full Birth Dates

We all love getting “happy birthdays” from our friends on our Facebook wall. It makes us feel all warm inside knowing that people remembered

and cared enough to write us a short note on our special day. The problem is when you list your birthday you are providing identity thieves with one of the 3 or 4 pieces of personal information that is needed to steal your identity. It's best to not list the date at all, but if you must, at least leave out the year. Your real friends should know this info anyway.

2. Your Relationship Status

Whether you are in a relationship or not, it may be best not to make it public knowledge. Stalkers would love to know that you just became newly single. If you change your status to "single" it gives them the green light they were looking for to resume stalking now that you're back on the market. It also lets them know that you might be home alone since your significant other is no longer around. Your best bet is to just leave this blank on your profile.

3. Your Current Location

There are a lot of people who love the location tagging feature on Facebook that allows them to let people know where they are 24/7. The problem is that you have just told everyone that you're on vacation (and not at your house). If you add how long your trip is then thieves know exactly how much time they have to rob you. My advice is not to provide your location at all. You can always upload your vacation pictures when you get home or text your friends to let them know how jealous they should be that you're sipping an umbrella drink while they toil away at work. Also disable GPS technology before taking photos with a Smartphone if you plan to post the photos online. Even some regular cameras have this technology, so check what information is included with your photos before posting them online. You should be able to turn off the high-tech feature before snapping, and you might want to consider doing so when you are in your home or places you frequent often.

4. The Fact That You Are Home Alone

It is extremely important that parents make sure their children never put the fact that they are home alone in their status. Again, you

wouldn’t walk into a room of strangers and tell them you are going to be all alone at your house so don’t do it on Facebook either. We may think that only our friends have access to our status, but we really have no idea who is reading it. Your friend may have had their account hacked or someone could be reading over their shoulder at the library. The best rule of thumb is not to put anything in your profile or status that you wouldn’t want a stranger to know. You may have the most stringent privacy settings possible, but if your friend’s account gets compromised than those settings go out the window.

5. Pictures of Your Kids Tagged With Their Names

We love our kids. We would do anything to keep them safe, but most people post hundreds of tagged pictures and videos of their kids to Facebook without even giving it a second thought. We even go so far as to replace our profile pictures with that of our children. Probably 9 out of 10 parents posted their child’s full name, and exact date and time of birth while they were still in the hospital after delivery. We post pictures of our kids and tag them and their friends, siblings, and other relatives. This kind of information could be used by predators to lure your child. They could use your child’s name and the names of their relatives and friends to build trust and convince them that they are not really a stranger because they know detailed information that allows them to build a rapport with your child. If you must post pictures of your children then you should at least remove personally identifying information such as their full names and birth dates. Untag them in pictures. Your real friends know their names anyway. If a friend or relative posts photos of your child on Facebook and you don't want them to, ask to take them down. After all, you don't know how carefully they monitor their own friend list, so it's impossible to know who is viewing the photos.

6. Watch out for lower-tech ways of sharing personal information, too. A photo taken in front of your home could reveal your address, or a T-shirt could contain a school logo. If you're posting photos on a blog or other public website, you probably want to keep your personal details under cover.

The bottom line: It's hard to control how your photos and information are used once they are posted online, but these steps can reduce your chances of becoming a victim of identify thieves or other criminals. The internet is really the new frontier. And just like the wild, wild west, it’s a free for all between the good guys and the bad guys with ordinary people caught in between. The best we can do is to circle the wagons and protect each other as best as we can. There are no foolproof methods but having a private site for your communications and sharing between close friends and family can be done on a secure website with more safety. See SitesTomorrow for more information regarding their Family and Friends Website Offer at SitesTomorrow.com.

Set your sights on tomorrow with SitesTomorrow.com