Social Media Privacy and Security

Social media provides many opportunities to connect with others, broadcast information, and share ideas online; however, there are also certain risks inherent to using social networks. By understanding and modifying your privacy settings, security settings, and user habits, you can minimize these risks and use social networks safely.

Although social network features may differ, they share several common security threats. Communications over social media are typically **unencrypted**, which means they can be read by anyone who intercepts them. **Impersonation** is also a major threat: without the correct security settings, it can be very easy for someone to gain access to your account by stealing your username and password. It is also possible for someone to impersonate your friend. On any social network, the **personal information** you post or send can become public if your account or a friend's account is compromised. Before posting sensitive information, consider this risk. You may also wish to use a pseudonym, although this violates the terms of service of Facebook and Google+. **Data on your computer** could also put you at risk, so make sure to manually delete sensitive conversations that are automatically logged, and avoid auto-login or password saving options. Additionally, social networks are frequently used to distribute **targeted malware** that may be disguised as fake login pages, links sent from unknown users or even friends, hidden links, and fake status updates. Although some of these covers may look suspicious, hackers are always coming up with new ways to make dangerous links and pages look more like regular social network activity. Before clicking anything, consider this risk and do not click anything that is sent from a user you do not know, an attachment you didn't expect to receive, an update available for download from an untrusted source, or a second login page after you have already logged in to your account.

Facebook

There are several recommended Facebook **security settings** that will better protect you and your account. Always use **HTTPS**, so that the information your computer sends to and receives from Facebook is encrypted. It is important to remember that Facebook messages and posts themselves are not encrypted and are not a secure way of communicating. (If you would like to chat with your Facebook account, you should do so using a secure chat protocol, such as Pidgin with OTR.) If you enable **login notifications**, you'll receive an email (or SMS, if you provide a mobile phone number) every time someone logs into your account from an unrecognized device. Although this will not prevent someone from accessing your account if they know your password, you will immediately know that someone is logging into your account.

Login approvals, also known as 2-step authentication, take this one step further. This feature, when enabled, will send a code to your mobile phone via SMS whenever you or someone else attempts to log in to your account. In order to successfully log in, you will not only need your password, but you will also need to input this code. Even if a hacker knows your password, he will be unable to log in without knowing the code sent to your phone. There are some risks involved with login approvals – if your mobile phone is registered in your name but your account isn't, your identity could be revealed. Additionally, if you lose your phone, it will be difficult to access your account. Facebook's **active sessions** feature allows you to see where your account is logged in. From this screen, you can end the activity of any session you don't recognize.

There are also some general security tips to follow when using Facebook. As mentioned previously, **look out for malware**, and remember that Facebook will only ask you to **login once per session** – any additional message asking you to login is most likely not Facebook and could be a hacker. Always **log out after every session** and keep your **browser up-to-date**, as newer versions will include updates to help protect you from scams and malware. Finally, only download applications and authorize apps from trusted sites and developers. Remember – Facebook apps can access your and your friends' Facebook information.

Another way to protect the information you post on Facebook is by updating your **privacy settings**. Before you update your settings, take the following questions into consideration: How much do you want others to know about you? What are you using Facebook for? Are you putting yourself and others at risk by sharing too much? If you are concerned about privacy, operate under the **less is more** rule. The less personal information you put on Facebook, the better off you are. If you never give it away, you've significantly decreased your risk! If you do decide to post something, privacy settings will allow you to **control who sees what**. Facebook allows you to group friends into different **lists** to determine and limit who can see what on your profile. Every photo album, wall post, and mobile upload should have a "Settings" option where you can select which lists you want to grant access to or block from viewing. You should also modify your privacy settings to limit who sees your profile information, wall/timeline, photos of you, and other content. Select "Friends," certain lists, or "Only Me" depending on how much you want others to see. Turning on **"Profile Review"** will allow you to review all posts, photos, status updates, etc. that you are tagged in – you will have to approve them before they are displayed on your profile. When posting **status updates**, be sure to delete your location so it is not listed automatically; you can also modify the settings of each status update so that only certain users can see them. Facebook also has a **limit audience for past posts** feature, which is a sort of "kill switch" that will allow you to limit who can see all of your past public posts to friends, a certain list, or even "only me."

Beware of default settings – many settings, when set to defaults, will share all of your information with the public. Facebook **messages** are also saved by default, so be sure to manually delete any that you do not want saved.

Protect your friends – When evaluating security threats, don't just think of yourself, think of your friends as well. If your account is hacked, will the identity of your friends be compromised? Will sensitive information on your account incriminate them? If you believe your account has been hacked, immediately contact your close friends and administrators of pages where you are active. This will give your friends the opportunity to un-friend and change their security settings if necessary, and will give administrators the chance to delete your admin privileges so that the hacker cannot hijack the page.

Be aware of Facebook policies – To promote accountability, Facebook has a real-name policy, which means that if you haven't used your real name on your account and your account gets compromised, Facebook will not restore your account. You should weigh the benefits of a pseudonym against the threat of losing your account when creating your Facebook account. Facebook policies also explain, "We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so." (For more information on this, visit https://www.facebook.com/about/privacy/other)

Facebook also routinely makes changes to their **privacy policy, default settings, and profile format** so be sure to keep up with these changes and read new policies. You should also routinely **check how your profile looks to your friends and to the public** to see if you are sharing more information than you think you are. You can check this by clicking "View As" on your profile.

If you'd like to delete your account, keep in mind that **deactivating** your account means it isn't viewable, but it still exists. **Deletion** takes up to a month and is permanent, but Facebook can still keep your information for up to 90 days after deletion.

Bottom line: If you don't put information on Facebook, it can't be shared. When in doubt, leave it out!

Twitter

To protect your **privacy and anonymity** on Twitter consider the following:

Who are you on Twitter? If you are tweeting controversial information or other content that could put you at risk, consider using a **pseudonym**.

What are you saying? You can chose to make your tweets **private**, so that only those you allow to follow you will be able to read them, unless you are re-tweeted. If you are using Twitter for advocacy, this will limit the number of people you will be able to reach. **Direct messages** are saved automatically, so you will have to review and delete what you do not want saved. You can only view 100 most recent direct messages; the rest are stored in a Twitter database, so be sure to delete sensitive messages immediately and often.

Where are you using Twitter? Make sure your settings are set up so that tweets don't include your location. You can also add or remove location information under the text box for composing a new tweet. To remove location information from all past tweets, go to your account settings and click the "Delete all location information" button.

How are you connecting to Twitter? Set **HTTPS** as default; use a **strong password**; watch out for suspicious links, messages, and emails; only allow 3rd party applications from sites you trust; and if you are concerned about security or are using a pseudonym, do not link your Twitter account to your mobile phone.

Using Twitter on your **mobile device** requires its own security assessment. Think about the tweets and messages that will be stored on your phone if you connect it with your Twitter account and the risks that this entails. Delete often from your phone! Be careful about giving away your **location** when tweeting from a mobile device, if doing so could compromise your security. For more information about using Twitter on your mobile device, visit support.twitter.com/groups/34-apps-sms-and-mobile

Consider the tradeoffs of using Twitter **anonymously** vs. using your **real identity**. Using your real identity may provide you with some **security** – if you send out an emergency message when you are arrested or attacked, people will immediately know you are in trouble and can respond accordingly. Using your real name may also give you a greater appearance of **legitimacy** if you are

using Twitter to conduct an advocacy campaign. However, using Twitter anonymously can give you a greater degree of **privacy**, and possibly **protection**, if you are tweeting about controversial issues.

In January 2012, Twitter announced it would start blocking tweets on a country-specific level. Although this is still **censorship**, it is an improvement on its previous policy, under which Twitter would have had to block these tweets globally. Additionally, the policy is **reactive, not proactive**: this means Twitter will only block tweets in response to requests from companies or governments relating to copyright law or local speech law violations. Twitter also made this policy relatively easy to circumvent; to access blocked tweets, all you have to do is change your country to a different one, under account settings. Twitter will publish information on blocking requests at www.chillingeffects.org/twitter and will identify any blocked content.

If you are worried about your or others' tweets being censored, you can **change your country** to somewhere different from where you actually are. This will also allow you to see tweets that may be blocked in your country and retweet or quote them to your followers, since blocking only applies to the original tweet and not to retweets. You can also attempt to avoid detection by **using clever wording** to refer to controversial topics. If one of your tweets is censored, you can **challenge the request** to Twitter directly.

Google

Due to a recent **Google** privacy policy update, all of your accounts for Google products and services (**Gmail**, **YouTube**, etc.) are linked under a single Google account. This policy also means that information you provide to ANY of these services will be associated with all other services on your account. Google also collects information on your activities on all Google services; this information is also associated with your account, and includes device-specific information, logging of content, location information, unique application numbers, cookies, and other anonymous identifiers. Additionally, records of your communications with Google regarding problems and issues you face will be linked with your account.

There are some steps you can take to respond to Google's Privacy Policy. Do not stay logged into any Google account as you browse the web, or **use a different browser** entirely (for example, surf the web with Firefox and use Chrome – with an "incognito" session – to manage your Gmail account). You can review a full list of your Google accounts and settings for all of them at **Google Dashboard** (www.google.com/dashboard/). You can also opt-out of personalized ads on Search, Gmail, and the Web, through **Google Ads Preferences** (www.google.com/ads/preferences/). You should also **edit your Google profile** to adjust what information you are sharing with Google and with the public (Note: the name on your Google Profile is the name that is used throughout ALL of your accounts). When posting to **Google+**, make sure to **use circles** to control what information you share with different groups of people (this is similar to Lists on Facebook).

Remember that Google **links your YouTube account** to a Google account. If you signed up for your YouTube account with a Gmail account, the two will automatically be linked. If you don't already have a linked YouTube account, Google will automatically create a YouTube account under any existing Google account that you have. When you sign into your Google account, you are **automatically** signed into YouTube as well. This is especially important to keep in mind when evaluating your account security and privacy – remember, you will not only need to update your YouTube account settings, but you will also need to update your Google account settings. To

increase your account security, we recommend the following settings: **Set up 2-step verification** — you will have to enter your password AND a code, sent by phone call or SMS, to login to your account. Do NOT connect accounts that use your real identity and accounts that use a pseudonym. **Provide an alternative email address** as a recovery option, in case you forget your password of your account is hacked.

If you are **setting up a YouTube account**, consider using a different Google account just for YouTube activities. If you choose to do this, you should use a Gmail address that you do NOT use often or that you do not use for important activities. This way, if the Google account linked to your YouTube account is compromised, the Gmail account you use for personal communications will still be secure. Remember that if you delete the Google account linked to your YouTube account, both the Google account AND the YouTube account will be deleted, and you will lose ALL videos and account data. However, you CAN delete a YouTube account without deleting the corresponding Google account (go to Settings > Manage account). Think carefully about what email address you provide, because you CANNOT change the email associated with a YouTube account if it is already under a Gmail account (because they will be linked).

A **history** of all the videos you view and everything you search for is automatically saved. You can, however, clear your history and pause recording of history. Your message history is also automatically saved, so you should delete anything that you want to keep private. Remember to be careful about what you share, and **avoid sharing personal information** on your profile. There is a **Privacy Complaint Process** that you can use if a video that shares personal information about you is posted on YouTube without your consent. This complaint process helps you to alert YouTube and request that the video be removed. You can also choose to make your channel **private** if you do not want it visible on YouTube.

Sharing allows your YouTube account activities to be posted on any other account you authorize, such as Twitter or Facebook. Only set up sharing to accounts that use the same identity that you have on YouTube (For example, avoid linking an anonymous Twitter account with a YouTube page that is under your real name). When you upload videos, you can choose to make them **private** or **unlisted**. **Private videos** are videos that only you and up to 50 people you invite can view; these videos will not appear on your profile, in search results, or in playlists. You must have a YouTube account to view private videos. People who know the link to the video are the only ones who can see **unlisted videos**. You control who can view the video by choosing with whom you share the link with. These videos will not appear in any of YouTube's public pages, including search results, on your channel, or in browsing. But be cautious; if someone you send the link to posts the unlisted video elsewhere on the Internet, it is no longer private! Be sure to tell your friends not to share the link or post it publicly. Your YouTube account must be in good standing to create unlisted videos. Other important YouTube settings include: **embedding** (you can enable and disable the option to allow your videos to be embedded) and **blocking** (you can block users from making comments on your videos or sending you messages by going to their channel page and clicking "Block user").

If you believe your account has been compromised, Facebook, Twitter, and YouTube all have ways to report the problem and ask for help.

- For Facebook, go to this website: https://www.facebook.com/hacked
- For Twitter, go to the Help Center > Report a Violation > My Account is Compromised/Hacked and I cant login

- For YouTube, go to the Help Center > Account Recovery

If these ways of asking for help do not work, please contact us for help at _____. (Contact information will be provided).

Resources

- **Facebook** - https://www.facebook.com/help/
- **Twitter** - https://support.twitter.com/
- **Google** - https://support.google.com/
- **"Me and My Shadow"** - http://myshadow.org/ – new Tactical Tech project that helps you determine your "digital shadow" (includes http://myshadow.org/lost-in-small-print , which shows visualizations of what you're really agreeing to when you accept Terms of Service (thus far only includes Twitter)