HOW TO:

ORGANIZE ON FACEBOOK SECURELY

POSTED BY SUSANNAH VILA IN DIGITAL SECURITY AND ANONYMITY, SOCIAL NETWORKING, FACEBOOK

More and more, people are using Facebook to gather online, spark conversations, share information and ideas, and ultimately meet offline. Sometimes it's for a protest, sometimes it's for a party; sometimes it's in a country where discussions of public life are discouraged or even punished and sometimes it's in a country where freedom of speech is a part of life.

Facebook is a potent tool, but to use it most effectively you should make sure that you're taking steps to minimize the chances of people seeing your communications who you do not want to see them.

This guide offers steps for doing so. Follow it to organize more safely, but know that even if you do everything we point out here, you should still be cautious and skeptical when you're organizing online and take your online interactions offline as soon as it is possible (and safe) to do so!

SHARE

RELATED HOW TOS

How To Recognize and Protect Yourself Against Email and Social Network Phishing


How To Use Your Mobile Phone Securely and Safely for Activism


How To Use Gmail More Securely


How To Improve Your Privacy and Security By Installing Tor On Your Android Smartphone


How To Browse the Web Safely and Securely Using HTTPS


How To Browse Facebook More Safely By Enabling HTTPS

How To Ask and Answer Questions with Quora

How to Curate and Create Stories from the Social Web Using Storify


How To Grow and Engage Your Facebook Base


How To Use Hashtags on Twitter to Spread, Share and Organize Information

BEFORE YOU DO ANYTHING ELSE

Step 1.

HTTPS. Using HTTPS means that you are creating a more secure channel over an unsecure network, better protecting you from surveillance and from someone accessing your web accounts without permission. Without getting too technical, HTTP stands for hypertext transfer protocol. It's a protocol that utilizes TCP to transfer hypertext requests and information between servers and browsers. **HTTP is unsecure** and is subject to interception, eavesdropping and surveillance. Using HTTPS, on the other hand, secures a webpage.

Right now, **HTTPS is not offered by default; users must opt-in by changing their settings**. To do so, go to: Account >> Account Settings >> Scroll down to Account Security >> Click change >> Check the box next to "Browse Facebook on a secure connection (https) whenever possible" >> Click Save.

Remember, though, that HTTPS does not mean that you will be completely protected, so don't throw caution to the wind just because you were smart enough to enable it!

Set a login alert. You will be emailed whenever a new computer or mobile device logs into your account. This way, if you get an email that your account has been accessed and it looks unfamiliar, you can find out if someone has breached your account. You might have already done this, because the checkbox for this setting is right below the box for enabling HTTPS. If you missed it, though, go to: Account >> Account Settings >> Scroll down to Account Security >> Click change >> Check the box next to "Send me an email" below "When a new computer or mobile device logs into this account" >> Click Save.

Step 2.

Prepare for a world without Facebook. Your content and your contacts are on Facebook's servers - not yours. So if your account gets deactivated by mistake or because you violated the company's Terms of Service, you'll lose all this information unless it's backed up.

Under Account Settings go to: "Download your information," then "Learn more," and then click on the download button. You can also get an Adobe Air application called SocialSafe or a Firefox extension called Archive Facebook which download

RELATED CASE STUDY

The Pink Chaddi Campaign

CONNECT ON FACEBOOK

FOLLOW ON TWITTER

RT @SMEXbeirut We're happy to announce MADskills, a new media TOT w/advocacy & development focus in #Lebanon. Apply now http://bit.ly/htqFyv
2 hours ago · reply · retweet · favorite

yes: Microsoft rep points out that tech platforms working on new products should be doing so based on what users want #yotech

your profile, social graph and photos onto your hard drive.

These will ***not download your contacts*** so save those somewhere else manually, as Egyptian activists running the We Are All Khaled Said page did in the weeks before internet access there was shut off.

PRIVACY SETTINGS

Step 1. **Understand the Facebook jargon.** Along with Facebook's growth has come **a whole new set of terms you need to know** in order to better understand what information the website is collecting and sharing about you. Here are some **common terms** used by Facebook to familiarize yourself with:

Public information: Facebook uses this term to describe information shared with anybody. **Your name, profile picture, gender, and networks do not have privacy settings and are visible to anyone.**

Visibility: What information can be seen by others looking at your profile. Remember: Some information can be seen by others that aren't your friends or even registered Facebook users.

Pages: Facebook pages are different from profiles. They usually are for non-user entities like companies, public figures, products, etc. The pages you are affiliated with (by "liking" a page) are available to anyone, including people you aren't friends with, advertisers, etc.

Connections: Created by "Liking" a page (clicking the "Like" button). This is considered public information.

Social plugins: Tools that are "dropped" into any website to extend the "Facebook" social experience to other sites. For example, if you are logged into Facebook and are browsing CNN.com, you may see a "Like" or "Recommend" button next to the article. If you "Recommend" the CNN article, a notification will be sent to your Facebook newsfeed that includes a link back to the CNN article. If you "Like" an item, the "Like" appears in your newsfeed and is also added to your "Likes and Interests" section on your Facebook profile.

Instant personalization: Lets you see relevant information about your friends the moment you arrive on select partner websites. Third party sites can give you a more personalized experience, which you may like, but it also

21 hours ago · reply · retweet · favorite

At #yotech @racheljo brings up the risks that @aym faces in engaging with activists around the world as an international NGO
22 hours ago · reply · retweet · favorite

The @Youtube revolutions: how the video uploading site has played a role in MENA protests http://bit.ly/g2dxp1
22 hours ago · reply · retweet · favorite

b
23 hours ago · reply · retweet · favorite

At #yotech, panelist reminds us that digital security education is about a lot more than just tools http://bit.ly/gK8EIt
23 hours ago · reply · retweet · favorite

thx :) RT @haleybowcock: Useful short 'how to' guide for planning a digital activism campaign http://is.gd/oRhB6m
23 hours ago · reply · retweet · favorite

RT @DigiDem: Our digital literacy manual is available for free! http://bit.ly/fiLr0l #yotech
yesterday · reply · retweet · favorite

@jilliancyork always here for that.
yesterday · reply · retweet · favorite

Do you follow us without receiving email updates on new online resources and events? That's silly: http://is.gd/f4Cjan
yesterday · reply · retweet · favorite

New Blog Post: Twitter's Still a Potent Force In Mexico http://bit.ly/gPUiHd
yesterday · reply · retweet · favorite

We're at Columbia U. today in #NYC to talk digital citizenship and youth @ewinstitute forum! #yotech
yesterday · reply · retweet · favorite

allows these sites access to your personal data. If you don't want to use Instant Personalization, visit your Facebook Privacy Settings page for Applications and Websites and uncheck the "Allow" check box next to "Instant Personalization."

Networks: You have the option of joining a school or workplace network on Facebook. One network will be your “primary” network - usually the network you feel most closely associated with. Your primary network will appear next to your name and influences which search results you see first. You can check what networks you have joined by going to the Networks tab of your Account Settings page. To join a network, you have to validate your affiliation with that particular college, high school or work network via an authenticated email address.

Step 2. **Understand what information Facebook collects about you when you interact with the platform.** Read Facebook's Privacy Policy and Privacy Guide.

According to the latest privacy policy (as of October 5, 2010), Facebook collects a variety of information, including:

- Information on your activities you take while on Facebook such as creating a photo album, adding a friend, “Liking” another user’s post, or sharing a video.

- Information from where you access Facebook from, whether it be from a compute or cell phone, including the browser you are using, your location and your IP address.

- Cookie information.

- Information from other Facebook users who interact with you, such as when a friend tags you in a photo of you.

Step 3. **Understand what information third parties collect about you** and what information those third parties share with Facebook. Third parties are applications or websites that you use through Facebook such as games or utilities.

When you connect with a Facebook Platform application or website, Facebook receives information from them about your actions. Facebook also may receive information from advertising partners if you respond to ads displayed on Facebook.

Step 4. If you live in a country where your online security is threatened, avoid using a

RT @jacobwe: China is cracking down while the world's attention is elsewhere RT @rmack No Word from Ai Weiwei in 24 Hours :: http://bit.ly/fuwtEu #aiww
yesterday · reply · retweet · favorite

Over the weekend protesters in Jordan kept momentum up with a new protest song, listen here: http://is.gd/ujgKHo #reformjo #24march
yesterday · reply · retweet · favorite

@TechChange @AU_SMCEDU @daryncambridge looks great sorry we arent there!
yesterday · reply · retweet · favorite

@AU_SMCEDU @daryncambridge @TechChange thanks for the shout outs! What's #sls11 ?
yesterday · reply · retweet · favorite

RT @habibh: The New Middle East belongs to its youth! #YallaStartup
3 days ago · reply · retweet · favorite

What are Nigerians saying about the upcoming election? http://is.gd/KqjGAf
3 days ago · reply · retweet · favorite

If you're in #NYC on Monday come to this event on youth digital security w/our @racheljo and @digidem 's @mbelinsky! http://is.gd/8MLFq7
3 days ago · reply · retweet · favorite

New Blog Post: How Social Media can Help Anti Corruption Advocacy In India http://bit.ly/gkxcHF
3 days ago · reply · retweet · favorite

RT @MorPerfectUnion: 8 steps for using #Hashtags better: http://j.mp/eDSmvM (via @aym)
4 days ago · reply · retweet · favorite

RT @Monajed: VIDEO: Security forces

picture of yourself as your profile photo, don't provide your full name, and **always log out when you are not using the site**.

To set your privacy controls? Log into Facebook. In the upper right-hand corner of any page, click on “Account” and then click "Privacy Settings."

Under the first heading, “Connecting on Facebook,” click the “View Settings” link.

You will then see a list of options for determining how much information you want to share on Facebook and with whom you want to share that information with. Next to each item you’ll see a brief description, and then **a drop-down menu where you can select your privacy preferences**.

You have four options: **Friends only** (only your approved Facebook friends can view this information), **Friends of Friends** (your Facebook friends and *their* friends can view this information), **Friends and Networks** (your approved Facebook friends and members of the Networks you have joined), and **Everyone** (*anyone* on the internet).

You also have **the option of customizing each privacy setting by selecting “Customize” from the drop-down menu**. This is helpful if you want to hide content from particular people. In the pop-up screen, you can customize the privacy of that particular information by making it visible to a select number of people you indicate or select networks. You can also choose to hide this information from particular Facebook users you have already added as friends.

Finally, **you can choose to make the information visible to “Only Me,” meaning that *no* friends can see that particular piece of information**. Set your preferences, then click “Save Setting” to return to the main privacy settings page.

On the main privacy settings page, click “Preview My Profile” to see what your profile looks like to your Facebook friends. This is a good way to double check that you have selected the settings you prefer. The website Reclaim Privacy provides an independent and open tool for scanning your Facebook privacy settings, but it's volunteer run and therefore not reliably up to date.

Tip!

Remember, even if no one but yourself can see certain bits of information, Facebook itself still has access to it - and you should not assume that they would

snipers on rooftops shooting peaceful protesters in #Syria http://bit.ly/iffpTH
4 days ago · reply · retweet · favorite

More Tweets | Follow us on Twitter

keep it to themselves were a government to ask them for it. Twitter was recently subpoenaed for user information, and although they not only challenged it but also told targets that their data was being requested, they didn't have to and you can't assume that Facebook or any other company would also do this. Also, as has happened recently in both Iran and Syria, security forces may detain you and force you to give up your password. In that scenario, they would login to your account have access to any information associated with your account regardless of privacy settings. So keep as little sensitive information as possible on the site.

Step 5. Under the second heading, "Sharing on Facebook," **set your preferences for who can see what information you share on Facebook**, including your status updates, photos and posts, your bio and quotations, your family and relationships, photos and videos you are tagged in by other users, religious and political views, birthday, permission to comment on posts you have made, places you check into using Facebook Places, and your contact information.

Again, you have the option of setting the sharing settings to Everyone (all registered Facebook users), Friends of Friends, or your Friends only. There are also Facebook's Recommended settings and then the option to customize your sharing settings.

By customizing your settings, you can set who can see and comment on items you share, things on your Wall and things you're tagged in. This is a nice option because for each piece of information you share you can determine who sees what. You also have the option to set certain bits of information to "Only Me," meaning that no one will see that information. Play around with the different settings; when you are finished click "Back to Privacy."

Step 6. Want to control how applications, games and websites access your information? Go to Account >> Privacy Settings >> Scroll to the bottom of the page >> Under "Applications and Websites" click "Edit your settings."

By default, applications have access to your friends list and any information you choose to share with everyone. Look through the list of settings for what information you share with applications and adjust your settings according to your preferences.

It's also a good idea to **remove any apps that you aren't using**.

Step 7. **Don't want your Facebook profile to be available on search engines when people search your name?** Go to: Account >> Privacy Settings >> Scroll to the bottom of the page >> Under "Applications and Websites" click "Edit your settings"

>> Scroll to the bottom of the page >> Next to Public Search click "Edit Settings" >> Uncheck the box next to "Enable public search."

Tip! Use this helpful webpage to search your Facebook information on Google.

Step 8. Are there particular users or applications you do NOT want to have access to your page? **You can block particular users or application invitations** by going to: Account >> Privacy Settings >> Scroll to the bottom of the page >> Under "Block Lists" click "Edit your lists." Add user names that you wish to block or the names of friends you want to block app invites from.

Step 9. **Some of your information may be available to apps, games, and websites when your friends use them**. To adjust these settings, go to: Account >> Privacy Settings >> Scroll to the bottom of the page >> Under “Applications and Websites" click “Edit your settings" >> Next to Info accessible through your friends click "Edit Settings." The pop-up box will ask you what information you want your friends apps and games to have access to. Uncheck the boxes next to the types of information you do not want your friends' apps to have access to.

Step 10. Remember to control your privacy settings when posting content onto your Facebook page. Each time you post something, such as a status update, a photo, or a link, **you have the options of controlling who sees the post**. Before you post a status update, link or anything else, click the lock icon at the end of the text field box to select who can see it.

Step 11. If you want to block Facebook plugins, download the Facebook Privacy List for Adblock Plus.

Step 12. Facebook Places lets you check into a particular location and share where you are with friends. Your Facebook friends can also check you into a location by tagging you. **If you do not want your friends to be able to check you into places, disable this feature**. Go to Account >> Privacy Settings >> Sharing on Facebook >> Customize Settings >> Friends can check me in to Places. Next to “Include me in "People Here Now" after I check in” uncheck the box next to “Enable."

Step 13. **You have to separately protect the visibility of photo albums** you upload to Facebook. Go to the Photos Privacy page and manually configure the privacy/visibility settings for each album you have uploaded.

Step 14. Facebook frequently makes changes to its privacy features, especially when they release a new product or service. Make sure to stay on top of changes at Facebook and take the time to review your privacy settings regularly.

Step 15. **Let your supporters know about how to best protect themselves on Facebook as well**. Share tips with them about how to adjust their privacy settings. *Have your own tip for maintaining privacy on Facebook? Share it in the comments section!*

Step 16. **It's a good idea to frequently back up your Facebook content and contacts** so that if your account is deactivated by mistake or because you violated the company's terms of service, you at least still have a copy of your information (including photos, messages, wall postings, and friend list). To do this, go to Account >> Account Settings >> Download your information >> Learn more. Click on the Download button. A pop-up will give you additional information. Click Download again. You will receive an email when your archive is ready to be downloaded as a zip file. It usually takes at least a few hours for Facebook to prepare the download. It's also a good idea to keep the minimum amount of sensitive information possible (for example, contact information) on the site at all. Why? Because you might have your password stolen or your account hacked into, and then it wouldn't matter what your privacy settings are.

Step 17. Are you very concerned about your privacy on Facebook, but don't want to delete your account? Some users are now trying the "super log-off." Each time you are finished with your Facebook session, **deactivate your Facebook account**. Then, when you want to log back on, just re-activate it. This does not delete your account; deactivation removes your profile and content associated with your account from Facebook. In addition, users will not be able to search for you or view any of your information.

To deactivate your account, navigate to the "Settings" tab on the Account Settings page. Reactivate your account by logging in with your email and password; your profile will be restored in its entirety.

PASSWORDS

As this BBC article notes, "**The majority of passwords people use adopt generic, often easy to detect patterns.** Knowing a bit of detail about someone, such as names of family and friends, favourite books and films, and where the individual lives, can often offer enough clues to successfully guess someone's password." Using a weak password is one of the easiest ways to make yourself and your accounts vulnerable online, choosing a strong one is also one of the simplest steps you can take to boost your online security.

Password cracking, the process of running computer programs against an

encrypted password in order to reveal it, is easier than you think. Programs that run every word in a dictionary or word list against a user name are also common. You can't totally ensure that your account will be protected from unwanted imposters (see our tips to avoid phishing, below) but there are some steps that you can keep in mind.

Step 1. The first step in creating strong passwords is to **know what weak passwords look like**. A weak password uses personal information, like your name, birthday, family member's names, or a pet's name. These types of passwords can easily be guessed by someone who knows you.

Tip! Can't come up with something original? Worried your password isn't strong enough? Try using an **automatic strong password generator** like this one. There are a variety of password generators out there - just Google and play around with them until you find one you like.

Step 2. Use Passphrases, not Passwords, and Keep Them Strong - passphrases are very similar to passwords, but are usually much longer and more complex. While a password may be six to ten characters, a passphrase is usually at least twenty to thirty characters in length.

Step 3. Learn what makes a password strong. A strong password is more secure and harder to break because it is **original, complex and random**. A strong password is also long, **containing at least 7 to 14 characters**, and **has a variety of characters**, including:

- UPPERCASE letters A-Z
- lowercase letters: a-z
- Numbers: 0-9
- Symbols: ~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/

Step 4. Come up with your strong passphrase. First, think of a few words or a sentence that comes to mind - it can be something completely random. Then **change some of the letters** to upper case and add in numbers, symbols and punctuation randomly (not just at the end of the phrase). It's also a good idea to **substitute a number or symbol for a letter**, such as using 3 for E.
For example, the song title "All You Need Is Love" becomes "ALuN##d57\./!." Also take the time to learn how to use Diceware to create a strong passphrase.

Step 5. **Check the strength** of your password on this Microsoft test site. Type in your password and the bar below the text box will illuminate with the password's

strength. Your password should reach "Medium" strength at a minimum. Keep tweaking your password until it's strong enough.

Step 6. Choose a password for your Facebook account that is exclusive to your Facebook account. It's not safe to use the same password for every site.

Tip! Keepass is a free and open-source password manager, making it easier for you to access your different passwords. It also stores all of your passwords in a highly secure database that is locked with one master key or key file. Now you don't have to worry about someone accessing your passwords.

Step 10. Other tips:

- **Never send your password to anyone over email.**
- Don't share your passwords with other people.
- Change your passwords every 3-6 months.
- **Try to avoid typing in your password on a public computer. If you must do so, change your password more regularly.**
- If you use Firefox for browsing, set up a master password.

DON'T GET PHISHED

(What is Phising?)

Step 1. - **Check the URL of the Facebook page**. Always log onto Facebook via a legitimate domain https://www.facebook.com. Don't log into Facebook if it is a similar but different domain. A fraudulent website may include the term Facebook before the domain (.com). This is called a subdomain. For instance, the address facebook.com.profile.a340ah3.com looks legitimate, but if you look more closely, the domain is actually a340ah3.com not facebook.com

- Be suspicious of any link, message, wall posting, or pop-up window that requires an additional login or asks you for your personal account information. Remember, **a phishing attempt could come from one of your Facebook friends** whose account has been compromised.

Step 2. **If you believe your account is being phished or you receive a suspicious link, message, post, or pop-up window that you believe is phishing:**

- **Report** it to Facebook by sending an email to privacy@facebook.com. Visit the

Facebook Help Center to get more specific help regarding your account.

- **Don't click on any links** in the post or message.

- **Never send sensitive personal information** like passwords, credit card information, or detailed personal information via a Facebook message.

- **Change your password** immediately. Learn how to create strong passwords and passphrases here.

- If the message or post comes from a Facebook friend, immediately **contact that person** to let them know that their account has been compromised. The same goes for a message or post coming from a company or oraganization you follow on Facebook.

- Share this knowledge with your friends!

Step 3. **Take the necessary steps to protect yourself against Facebook phishing in the future:**

- Remember to have **enabled HTTPS.** In the case of Tunisia, experts found that the embedded JavaScript only appears when Facebook was accessed with HTTP instead of HTTPS, underscoring the importance of using HTTPS whenever you log into social networking sites.

- Always make sure you are logging onto Facebook via a legitimate domain.

Step 4. If you have given out your personal information and believe you've been the victim of phishing, check out the Anti-Phishing Working Group's advice on what to do.

ANONYMITY

Step 1. Facebook's Terms of Service includes a real name policy prohibiting joiners from using pseudonyms. That said, plenty of people do.

The site's crackdown on these users has been arbitrary and erratic, so if you create a fake name on Facebook avoid getting kicked off by making it a convincing one rather than an obvious (one word) pseudonym, and most importantly have a plan of action in place in the event that your account does get deactivated.

Part of your plan of action should include learning the Terms of Service (TOS) ***so you know if you violated it or not***, as well as how violations get reported (by other

users, which can be abused). If you don't have time for this, then get in touch with someone who does and who has the time and resources to contact Facebook directly on your behalf. Try info@movements.org.

Step 2.

Anonymity is about more than simply first and last names.

What other information might identify you? Is your phone number public? Is there a picture of you next to an identifiable landmark in the neighborhood where you live? (You should ***avoid using an actual picture of yourself as your profile photo in the first place)***.

What about the people you've friended? A close connection on Facebook to someone who has been arrested for political activism, or is involved with a group that you don't want to be associated with, may get you in trouble, so be careful about who you friend and watch who you're connected to using tools that allow you to analyze your networks - for example Friend Wheel or Social Graph. If Facebook privacy settings have got you confused, remember you can always preview how your profile looks to others, and what information you're exposing, by going to "Account," "Privacy Settings," "Customize Settings," "Preview my profile(see below picture)."

Step 3

General tips for anonymous browsing apply to Facebook use, so check out our guides on:

- Blogging anonymously with Tor
- Using Gmail securely
- Using your mobile phone safely and securely
- Protecting your identity while you surf the web using Hotspot Shield
- Improve your security on your Android phone by installing Tor

SHARE

SHARE YOUR LESSONS LEARNED AND SUGGESTIONS!

DISQUS