Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email
usarmy.cciuintel@mail.mil

CCIU Web Page
http://www.cid.army.mil/701st.html#sec6

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:
This document is authorized for wide release with no restrictions.

"DO WHAT HAS TO BE DONE"

CPF 00004-16-CID361-9H-Facebook*   8 March 2017

## Configuring Facebook for a More Secure Social Networking Experience

Settings

Settings are available under the Facebook Configuration Arrow.

General Account Settings

Name

You can change the name of your Facebook account to just about anything; however, Facebook's rules require that the name be your actual name. In Facebook's own words, "Facebook is a community where everyone uses the name they go by in everyday life. This makes it so that you always know who you're connecting with and helps keep our community safe." Facebook, and likely every other social networking site, does not make a serious effort to verify anyone's identity.
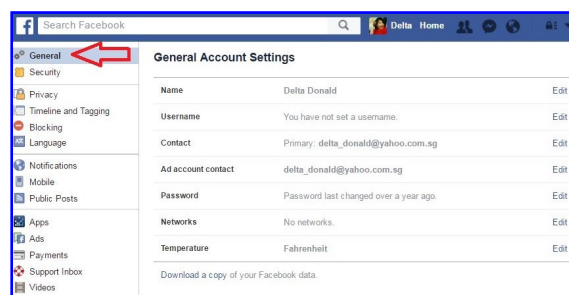
The alternate name feature can be used for an unmarried name so friends can locate you (e.g., Susan Smith (Jones) or a nickname or diminutive of your given name). Once a name change is made, you are required to wait a period of time before another name change can be made.
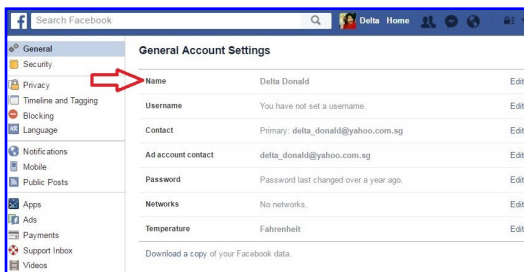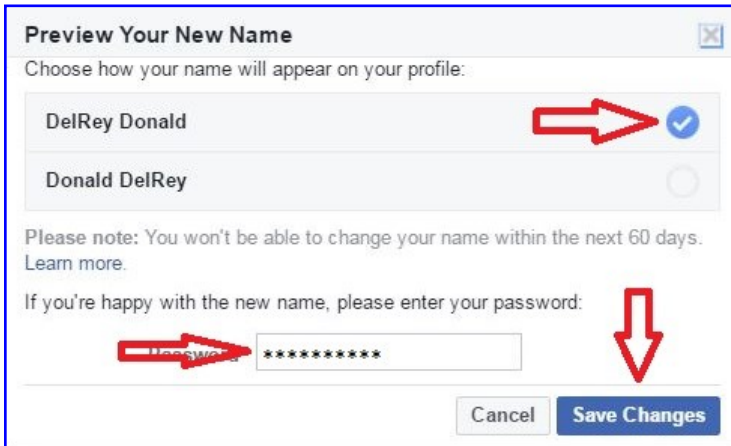

1. Click **Name**.

2. Make changes as necessary and click **Review Change**.

---

* This Facebook configuration guide supersedes CID Crime Prevention Flyer CPF-00009-15-CID361-9H.
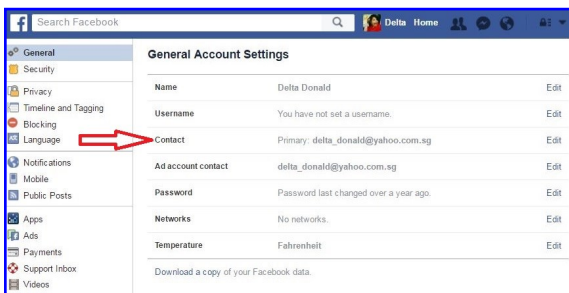
3. Facebook presents a preview of how your name change will appear on your timeline.

4. Check an acceptable variant, enter your password, and click **Save Changes**.

Email

When you created your Facebook account, your registration was verified through email or text message. That means that Facebook sent an email message to the email address you provided. That email message had a web link you had to click to verify your email address.

This is also where you change your email address if the address you registered with Facebook is disabled or retired for any reason or if you want to receive emails in a different mailbox.
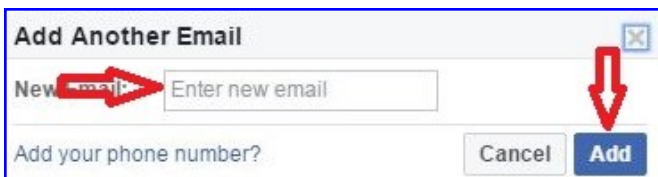
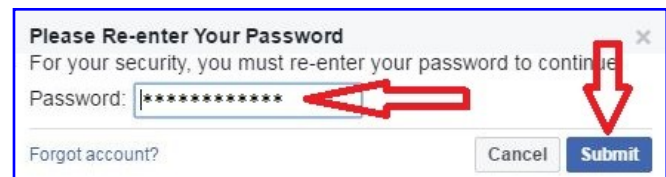To change your email, from the General Account Settings menu:
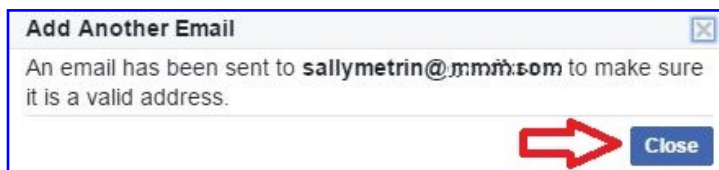

1. Click **Contact**.

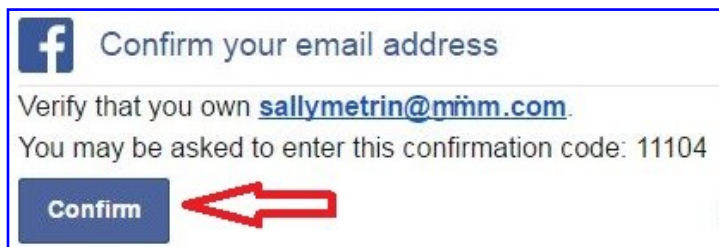2. Click **Add another email or mobile number**.

3. Enter the new **email address** in the box.
4. Click **Add**.

5. Enter your password and click **Submit**.

6. Click **Close**.
7. Facebook will send an email message to the new email address confirming the change and a notification of the change to the email address of record.


8. Check for email at the new email address. It will look like this. Click **Confirm**.

9. Return to the General Settings area. If you see this message, the changes were successful.

Delete an Existing Email

Facebook will not allow the removal of an email if it is the primary email or it is the only email. If you do not have a secondary email, you must add one. Follow the instructions in the section immediately above to add a secondary email address. Then, to delete an email address, from the General Settings menu:
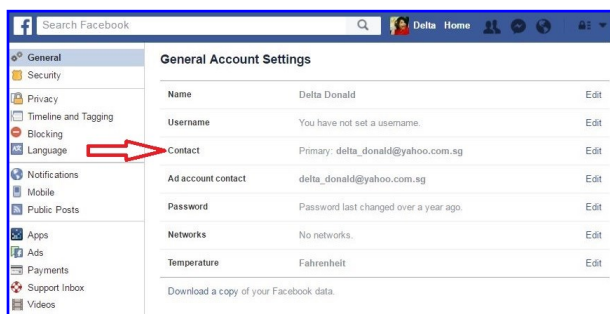
1. Click **Contact**.

2. Click **Remove** next to the address you want to remove.
3. Click **Save Changes**. If you have chosen to remove an email address and save changes, you will receive an email at the removed email address notifying you of the change.
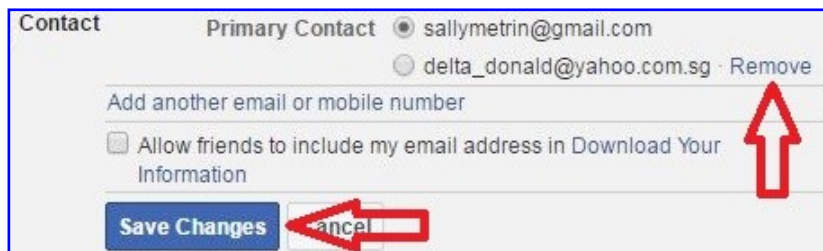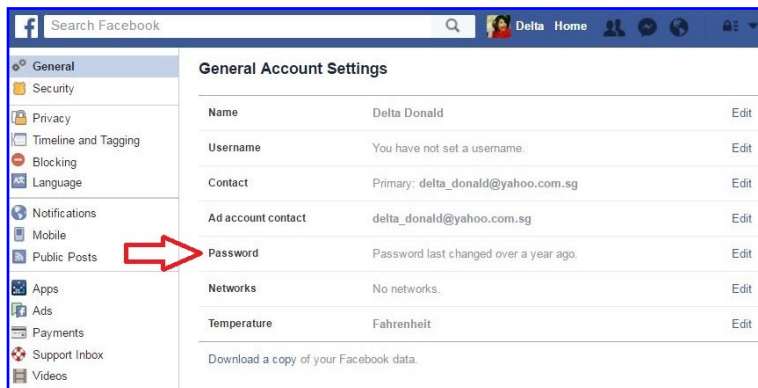
Passwords

Passwords, secret elements of authentication, are on the front line of defense preventing people and automated tools from illegally accessing your online accounts. Therefore, your choice of password and the frequency with which you change it are important security considerations.

A password, however, need not be limited to a word. It can be a passphrase. A passphrase is a string of characters that form a phrase. An example might be, "The song remains the same" or "I'll see you on the dark side of the moon". Passphrases are generally easier to remember than complex passwords and more likely to survive a dictionary attack than is a password.

Guidelines for passwords to avoid, especially if you are a public figure or in a situation where much of your personal information is in the public domain, include:

- Your name or any permutation of your name
- Your user ID or any part of your user ID
- Common names
- The name of any relative, child, or pet
- Your telephone number, social security number, date of birth, or any combinations or permutations of those
- Vehicle license plate numbers, makes, or models
- The school you attended
- Work affiliation
- The word "password" or permutations including "password" prefixed or suffixed with numbers or symbols
- Common words from dictionaries, including foreign languages
- Common dictionary word permutations
- Names or types of favorite objects
- All the same digits or all the same letters or letter sequences found on keyboards (e.g., QWERTY)

1. Click **Password**.

2. Enter your current password.
3. Enter your new password or passphrase.
4. Re-enter it for verification.
5. Click **Save Changes**.

Security Settings

Security Settings are available under the Facebook Configuration Arrow.

Login Alerts

This is an effective means to identify attempted compromises to your Facebook profile. When accessing your profile, after correctly entering the username/password combination, Facebook checks for the presence of a cookie on your computer. That cookie identifies the browser as one from which you have accessed Facebook before. If the cookie is found, the login proceeds without further interaction.

If the cookie is absent or incorrect, Facebook will ask the user if information about the browser should be saved AND sends a text message or email to the addresses of record indicating a login from an unknown browser.

If you elect to use text messages, you will be required to provide Facebook with the number of your mobile device. This presents a separate issue. See the section labeled **Who Can Look Me Up**.

If this browser is unrecognized, you will encounter a Facebook challenge asking if you want to **Remember Browser**. Do not save that browser information unless you are using a computer you have control over and will use again. If by chance you mistakenly opt to save the browser or there is a browser you have previously saved but know you will not use again in the future, you can delete that browser by following the instructions in the section **Recognized Devices**.

Login Alerts is not double authentication. If the correct username/password combination is entered, the user will be allowed access to the profile. The defensive benefit of **Login Alerts** is the email or text message notifying you of the access. If you receive a login alert and did not log in, you should immediately change your password and take immediate steps as outlined in the sections **Recognized Devices** and **Where You're Logged In**.

Login Alerts will not work if your browser is configured to refuse cookies or if your browser clears its cache when it closes. If your browser is set to refuse cookies or clear cache when exiting, it is best to leave these settings as they are and not use the **Login Alerts** feature.
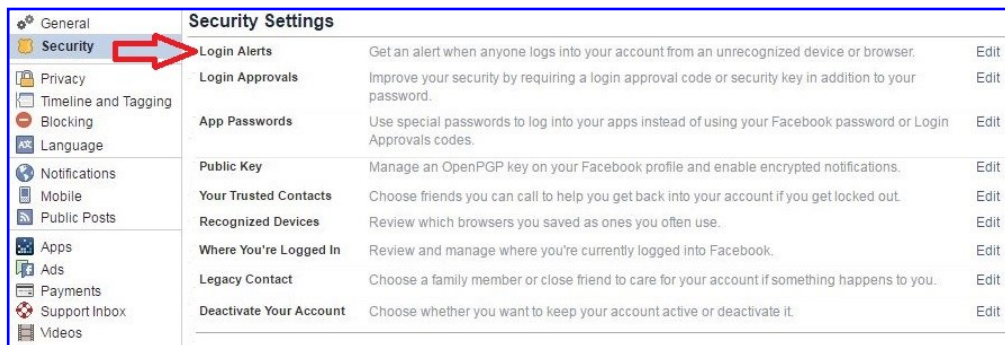
1. Click **Login Alerts**.

2. Select **Get notifications**.
3. Select **Email** and click **Save Changes**.
4. Email notices will be sent to your email on file with Facebook.
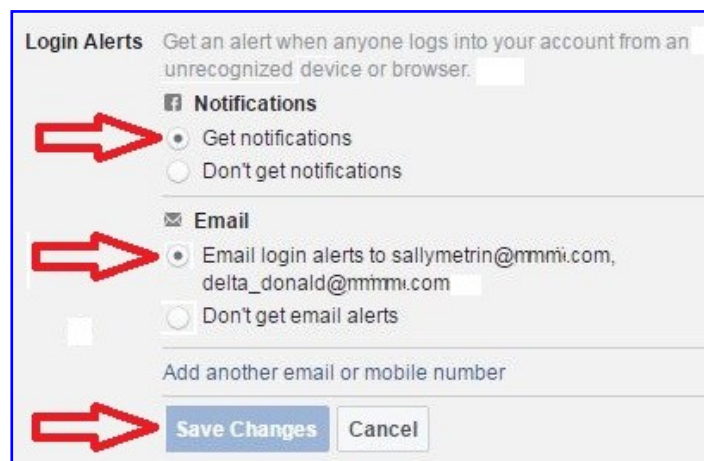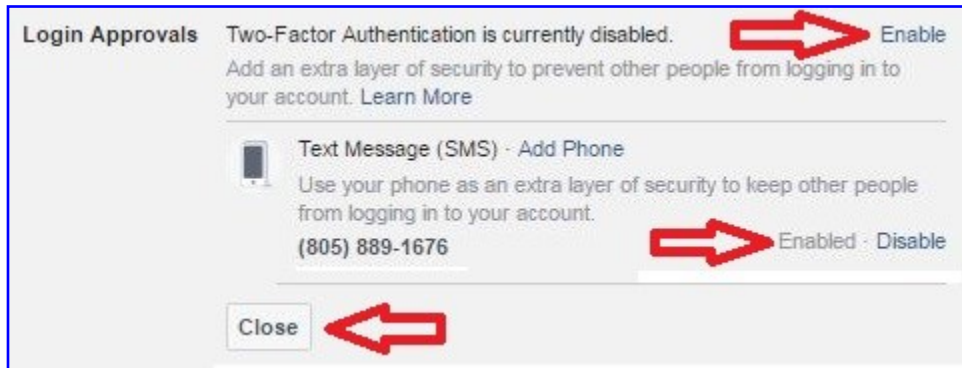
Login Approvals

This is the best way to prevent your Facebook account from being accessed by someone else. Every login attempt to your Facebook account will be interrupted and a code sent to the mobile phone on file with Facebook. Only after that code is correctly entered into the Facebook dialog box will the login proceed past the challenge screen. The recipient of the text message has 20 seconds within which the login must be completed or the code expires and the process must be repeated.

Login Approvals, in conjunction with **Login Alerts**, will provide a substantial level of protection against profile compromise.

> *WARNING—If you use Login Approvals and retire the mobile telephone number without first updating the default number in Facebook you will likely lock you out of your account forever. Facebook support might not be able to help you.*

1. Click **Login Approvals**.

Cybercrime Prevention Flyer
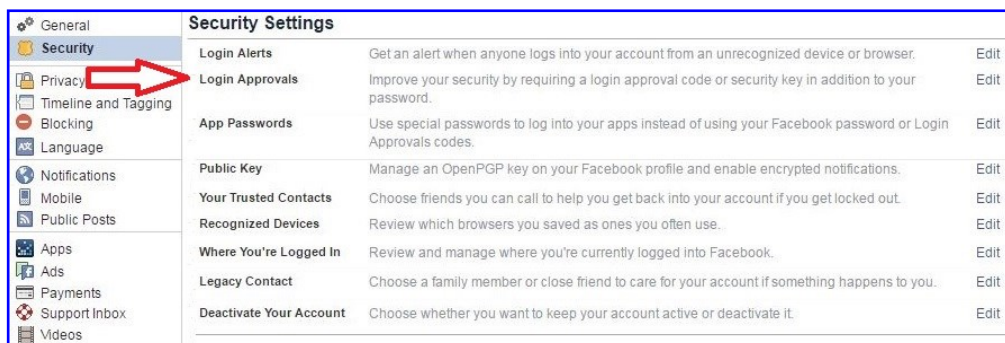
2. Click **Enable** to start Login Approvals.
3. Click **Enable** to use the mobile phone on file with Facebook.
4. Click **Close**.
5. Check your mobile phone for a verification text message. Follow the instructions in that message.

Your Trusted Contacts

Facebook friends you can contact to help you access your Facebook account if you get locked out are trusted contacts. When you select your trusted contacts, they will receive notification that they are trusted contacts so it is best to notify them prior to enabling this feature.

Trusted contacts should be people you know well - people you can trust. Your trusted friends should be familiar with their responsibilities and understand that if they are ever called upon to assist you, they should verify absolutely it is you asking for their assistance. Accordingly, email is probably a poor method of verifying identity.

If at any time you decide you no longer want to have trusted Facebook contacts or you decide one or more of your trusted contacts can no longer be trusted, you can make those modifications in the **Trusted Contacts** area of security settings. Dropping a trusted contact does not generate an email message to the dropped friend.
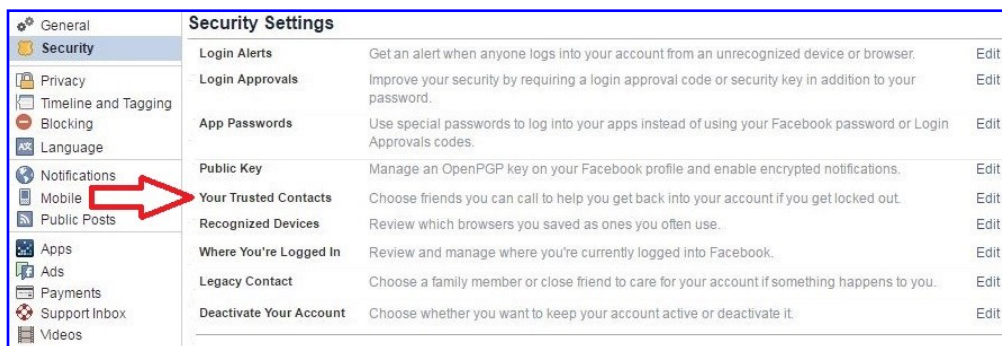
Regardless of the trusted contacts you add or remove, you cannot have more than five nor less than three.

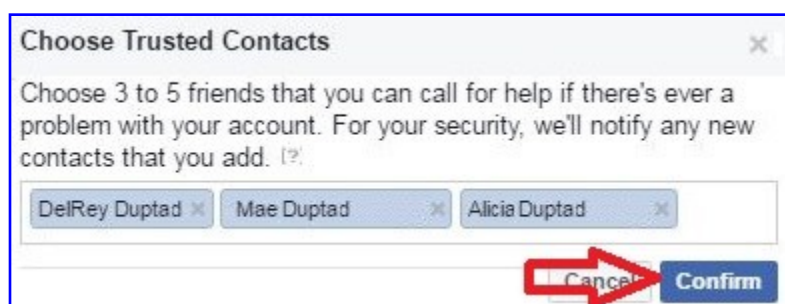1. Click **Your Trusted Contacts**.
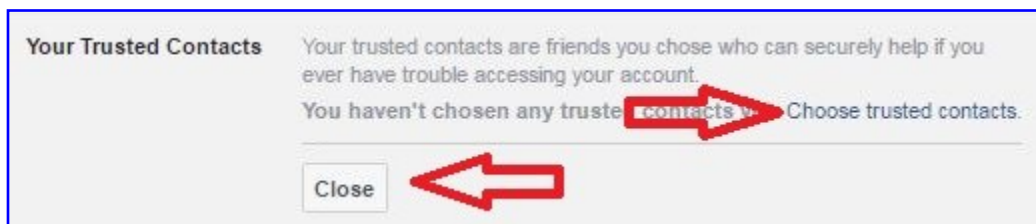
2. Click **Choose Trusted Contacts**.
3. Click **Close**.
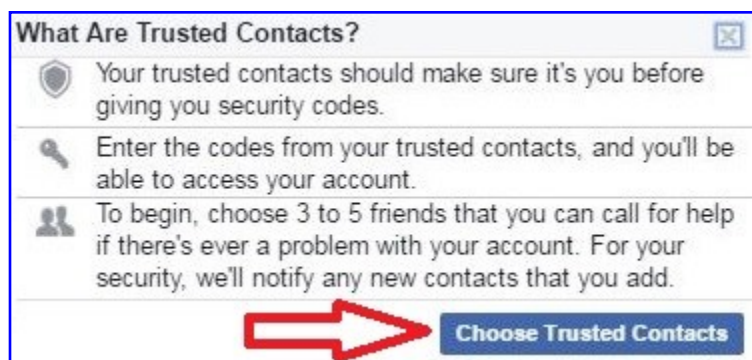
4. Read this statement carefully.
5. Click **Choose Trusted Contacts**.

6. Add from three to five trusted friends. These trusted friends must already be in your Facebook friends list.

7. Click **Confirm**.
8. Review your choices and click **Close**.

Where You're Logged In

This feature can be used to end any active Facebook session, including the one from which you are accessing your Facebook account. Like **Recognized Devices**, this is more of a security audit tool than a security measure. **Where You're Logged In** will identify those computers from which you might not have properly logged out of Facebook and can tell you if unauthorized access to your account has occurred.

A generally good security practice is to log out of any internet activity that requires a login; logging out is a specific menu choice. Closing the browser or restarting the computer may be insufficient to fully log out. In some circumstances, like accessing your Facebook account from a public computer or any computer that multiple people use, simply closing the browser window will not log out of Facebook. Then, quite possibly, the next person who opens Facebook from that computer could open to your account without being challenged for a password, giving them unintended full access.

If you see a logged in browser and believe it to be an unauthorized connection you should:

- End the session associated with that browser,
- Change your password,
- Check **Recognized Devices** (see below) and remove any improperly authorized browsers,
- Recheck **Where You're Logged In** to verify that a new session was not started.
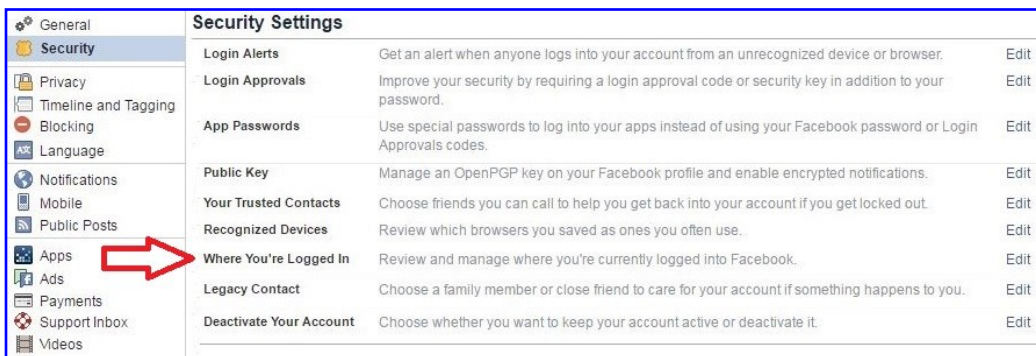
1. Click **Where You're Logged In**.
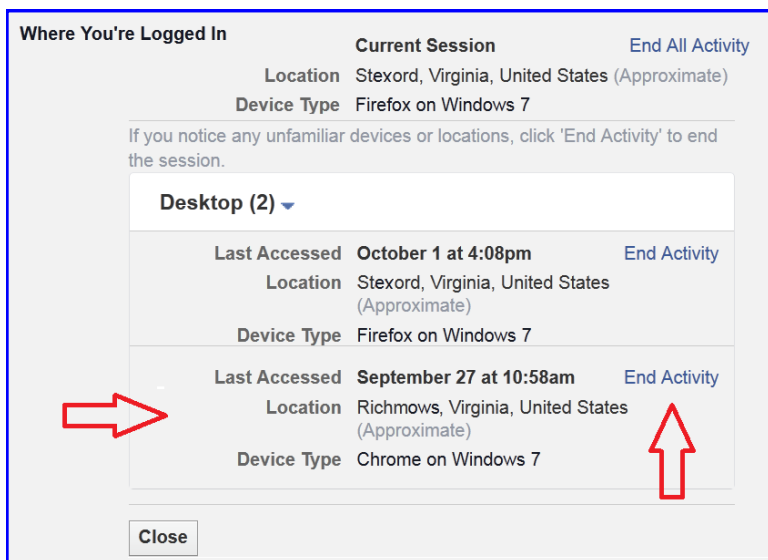
2. Identify locations where you want to end activity and click **End Activity**.
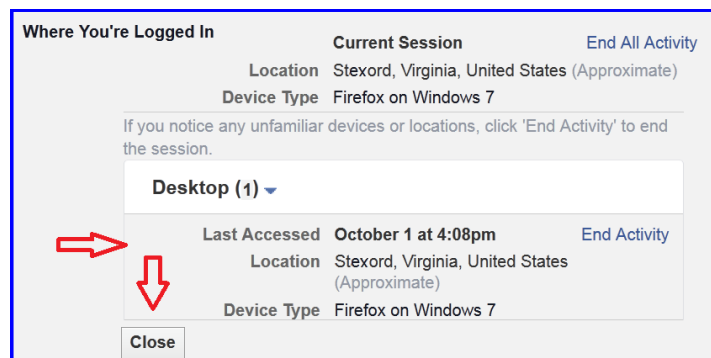
3. Verify that the session ended then click **Close**.

Recognized Devices

Not so much a security setting as it is an audit tool, the list of **Recognized Devices** shows you the browsers with which trusted relationship have been established, the corresponding operating system of the machine the browser is installed on and the date trust was established.

If you use **Login Alerts** then you should occasionally check this list and remove any browser you no longer use, **Recognized Devices** you suspect are being used by others to access your account (this forces a login notification email the next time anyone logs in), and browsers you may have mistakenly trusted.

If you see a browser listed as a trusted browser you do not recognize, you should:
- Remove the browser
- Change your password
- Check **Where You're Logged In** (see above) and end activity that is not you
- Recheck **Recognized Devices** to verify that a new trusted browser has not been added
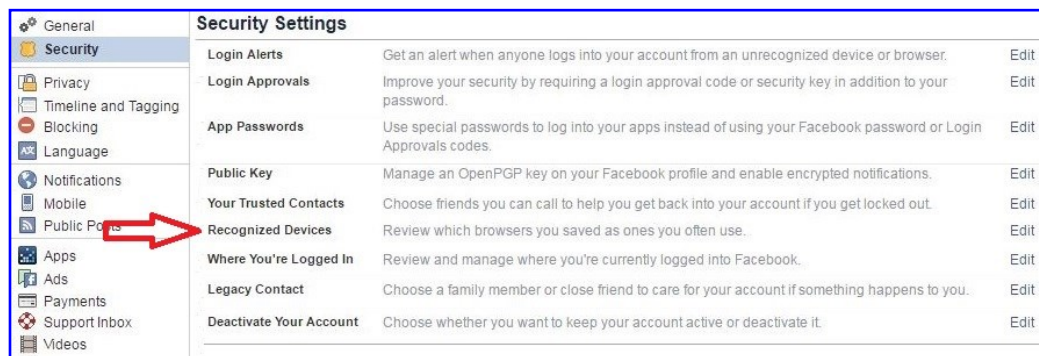
1. Click **Recognized Devices**.

2. Identify the browser you want to untrust.
3. Click **Remove** opposite the unwanted browser.

4. Verify that the intended browser is about to be removed. The browser that is about to be removed will have **Undo** next to it.
5. Click **Save Changes**.

Privacy

Who Can See My Future Posts

Limiting the visibility of future posts to just friends is the best way to limit access to items on your timeline to people with whom you have a trust relationship. This assumes that people on your friends list are in fact the people they purport to be. Social engineering is a reality and Facebook does not make a serious effort to verify the identity of new subscribers.
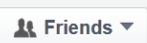
1. Click **Who Can See Your Future Posts?**

2. Click the selection down arrow.
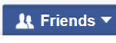
3. Select **Friends**. 4. Click **Close**.

WARNING—Changes made here will automatically and without warning change the global setting of Who Can See My Future Posts!!!

You can override this setting for an individual post by clicking on the audience button and selecting the desired option.

Limit the Audience for Old Posts on Your Timeline
This setting is powerful and immediate. Read the onscreen information and be sure you understand it before you execute it. If you have opted to make all future posts visible to friends only then it does not make sense to not make all past posts visible to friends only as well.

This option changes the setting on *all* posts already on your timeline so they are visible *only* to your friends. The only change option is to friends. Once executed, the only way to undo the changes is by changing the **Who Can See This Post** on each timeline item.

1. Click **Limit the Audience for Posts You've Shared with Friends of Friends or Public**.

2. Click **Limit Old Posts** and the click **Close**.

    The outcome of this option is that ALL past posts on your timeline will be changed to **friends** only. There is no means to select any other outcome than **friends**.

Who Can Look You Up Using the Email You Provided?
                                      and
Who Can Look You Up Using the Phone Number You Provided?
In order to create a Facebook account users *must* provide a valid email address or mobile number. The email address is verified when Facebook sends an email that contains a link the user must click in order to demonstrate the validity of the email address.

The mobile phone number is verified when Facebook sends a text message that contains a verification code and that code is entered into Facebook a verification dialog.

However, these small steps of validation should not be interpreted to mean that Facebook user identities are properly vetted. Anyone can use any of the free email providers to create a "single use" email address or one of the available online disposable phone number sites to receive text messages. This creates circular verification - a fake email address or mobile number to verify a fake social media account.

If you have enabled **Login Alerts** using text messaging, login approvals, or code generator then you have provided Facebook with your telephone number.

Regardless of how Facebook obtained your email or telephone number, it could be possible for any Facebook user to locate your profile using only your email address or telephone number. This option should be turned off for both contact methods.

1. Click **Who Can Look You Up Using the Email Address You Provided?**

2. Change the setting to **Friends** (the most restrictive).
3. Click **Close**.
4. Execute the same steps for **Who Can Look You Up Using the Phone Number You Provided?**

Do You Want Other Search Engines to Link to Your Timeline?
Your profile can be located using most internet search engines and parts of your timeline may be visible even to those without a Facebook profile. By controlling this setting, you can reduce the possibility of your Facebook profile being located by someone other than a Facebook user.

Users must bear in mind that, for some considerable but indeterminate period of time after the search capability is turned off, residual records in a search engine will persist.

1. Click **Do you want search engines outside of Facebook to link to your profile?**

* **Outside Search Engines** refers to search engines other than the search capabilities provided within Facebook.

2. Deselect **Allow search engines outside of Facebook to link to your profile**.
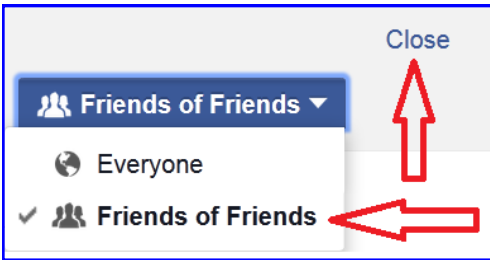3. Click **Close**.

Who Can Send You Friend Requests?

Limiting the people who can send you friend requests to friends of friends provides a little extra assurance that a friend request is coming from someone in your personal network. But be cautious! Accepting a friend request from someone you do not know simply because they are a friend of a friend effectively pushes the burden of vetting new requests to your friends; their efforts might not be commensurate with the level of verification and protection your identity requires.

1. Click **Who Can Send You Friend Requests?**

2. Click **Friends of Friends** (the most restrictive).
3. Click **Close**.

Download a Copy of Your Facebook Activity

You might find yourself in a situation where you would like to review all of your Facebook activity. Maybe you want an archive of all images you've posted to Facebook but didn't save to your local computer. Fortunately, there is a way to do this without scrolling through innumerable Facebook pages. You can download to your local computer a copy of your Facebook data.

A word of caution—DO NOT download a copy of your data to any computer you do not have total ownership of. Do not download your data to a borrowed computer, a public computer like those you might use at a library, community center or school, or your work computer.

Before you start the download process, consider the following:

- The time required to create your downloadable content could take hours or possibly days.
- The downloadable file could be many gigabytes or even many, many gigabytes. It will be large.
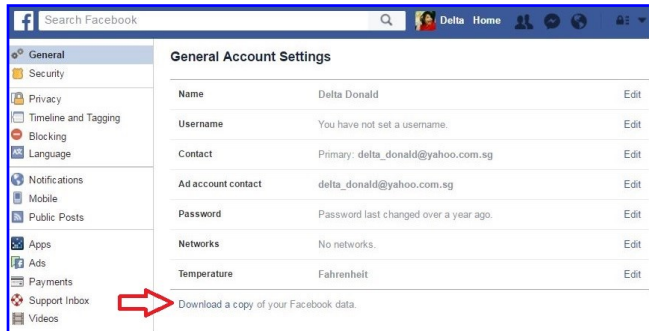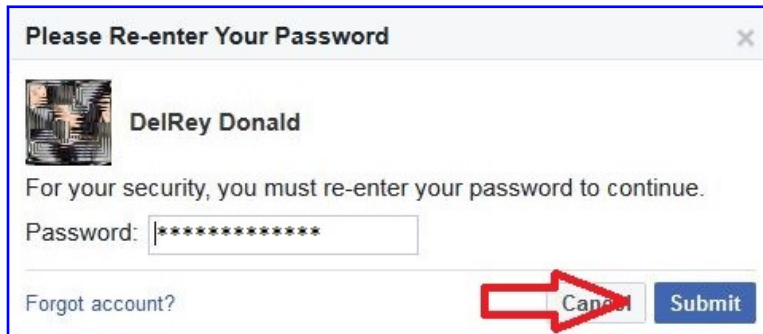

1. Click **Download a Copy of Your Facebook Data**.
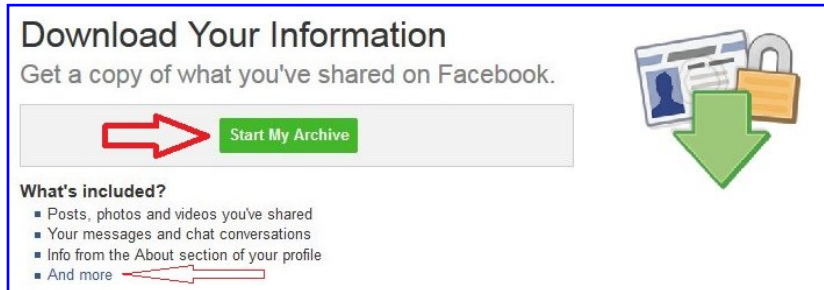
2. Click **Start My Archive**.

   (Clicking **And More**, at the bottom of this dialog box provides, an idea of the content you can expect. You can click this link while your download is being prepared. A better plan is to look at it before you start your archive. It will give you insight into how big the download could be.)

3. Enter your password to confirm your identity.
4. Click **Submit**.

5. Click **Start My Archive**.

6. Click **Okay**.
7. Periodically check your email account for a Facebook notification that your archive is complete.

8. Review the statement in the Facebook email and click the hyperlink.

9. Click **Download Archive**.

10. Enter your password and click **Submit**.
11. To complete the download process you will need to navigate through several more dialog boxes. Follow your operating system's procedures for saving the archive file.

The downloaded file will be compressed (e.g., zip). Save the contents of the compressed file to a new folder. Your data will be arranged in more subfolders named for the content (e.g., profile, contact info, timeline).

Return to <u>Social Networking Safety Tips</u>

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to <u>provide</u> us with feedback.

The Army's Digital Detectives