Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

**27130 Telegraph Road
Quantico, Virginia 22134**

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"DO WHAT HAS TO BE DONE"

CPF 00012-2020-CID361-9H   19 August 2020

Configuring LinkedIn for a More Secure Professional Networking Experience

Things to Consider Before Using LinkedIn

LinkedIn is more than just a social networking site; it is a social networking site for professionals. LinkedIn is for the adult professional seeking to network with similarly situated adults, all of whom are building professional networks and developing business associations. LinkedIn is not Facebook, Twitter or Instagram. If you are on LinkedIn, it is because you want to be identified as a professional and you want people to know about your professional background. If this is not the case, perhaps you do not need a LinkedIn presence.

> *The key is to keep company only with people who uplift you, whose presence calls forth your best.*
> Epictetus

Configuring LinkedIn for maximum safety is challenging. Users must decide how to balance privacy, security and safety against the value of building a successful business network. Accordingly, the configurations in this Cybercrime Prevention Flyer are recommendations. Most of these recommendations will not apply if you are using the account as a representative of an organization.

Regardless of how effectively and completely you control LinkedIn settings, there is no way to completely hide yourself. You can reduce your exposure but you cannot be invisible. (If hiding or being invisible is your goal, then you probably do not want or need a LinkedIn presence.) Unless you change the default settings on your public profile, it will be visible even to those who are not LinkedIn members and your information will be indexed by search engines. As a general rule, do not put anything in your public profile you do not want the world to know. Do not put things like email addresses, telephone numbers or physical addresses anywhere but in fields labeled for that information.

Identity Verification
LinkedIn has varying levels of user identity authentication, none of which guarantee the LinkedIn member is the person their profile purports them to be. With the free basic membership, all that is required to join LinkedIn is a valid email address. LinkedIn verifies the email address by sending a verification email. When the recipient clicks an included link, the email address is verified. However, valid email addresses can be obtained from any of a number of free and completely anonymous email providers.

LinkedIn does offer paid memberships tailored to various needs and these require a credit or debit card against which LinkedIn charges membership fees. Nonetheless, untraceable gift cards are readily available and look and operate like credit cards.

So, in reality, anyone with an intention to deceive can, with minimal effort, obtain a LinkedIn membership. This is not to suggest that LinkedIn is riddled with impostors. Quite the contrary, LinkedIn has hundreds of millions of members, like you, using the site for legitimate purposes. Just be careful.

Making Connections
Making connections is how you build your professional network and your credibility. Connecting with you is how others build their networks and their credibility. If we are judged by the company we keep, then deciding to accept, decline, block or report a connection request is an important decision. Likewise, with whom we seek connection is equally important.

Since LinkedIn attracts professionals, people in positions of responsibility and trust, like you, its members may be more attractive targets for criminals. Therefore, you should consider the following:
- Do not include in your profile that you have a security clearance.
- Exercise appropriate skepticism when contacted by someone not known to you regardless of how credible their LinkedIn presence appears. Not everyone on the internet is who they say they are.
- Be cautious when considering a connection request because the requestor's network includes people you know only tangentially.
- Seek and accept connections that add quality to your professional network and consider the ramifications of accepting connections that do not.
- Do not accept connection requests based entirely on the strength of the requestor's network. People sometimes build false networks and leverage their false credibility to more easily facilitate social engineering.

Accessing Your LinkedIn Profile Settings

LinkedIn profile settings are accessible along the command ribbon beneath your profile picture.

Settings and Privacy
To access **Settings & Privacy**, click the dropdown arrow under your profile picture next to the menu option **Me**. When the **Account** menu appears, click **Settings & Privacy**.

Controlling Access to Your LinkedIn Account

Passwords
Passwords, secret elements of authentication, are on the front line of defense preventing people and automated tools (e.g., password crackers) from illegally accessing your online accounts.

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 are more likely to survive a **dictionary attack** than is a single word.

Changing passwords is a straightforward process. A good practice is to change your password from time to time and is an absolute necessity if you believe your profile has been compromised.

Guidelines for passwords to avoid, especially if you are a public figure or in a situation where much of your personal information might be 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 a keyboard

To change your password, from the **Settings & Privacy** menu,
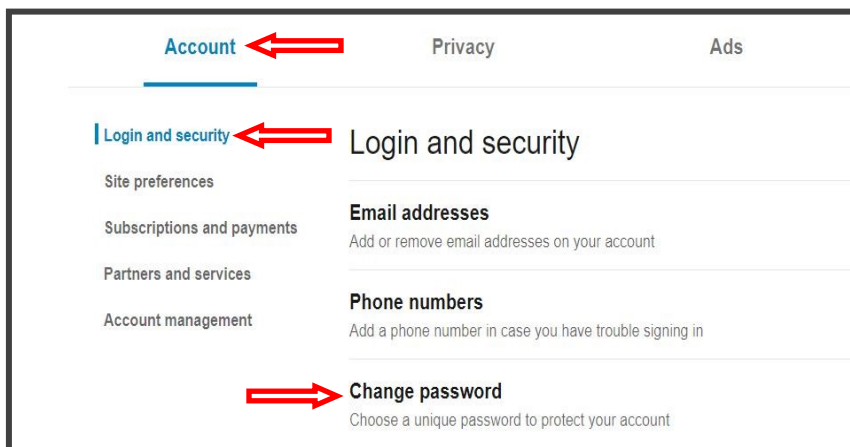
1. Click the **Account** tab.
2. Click **Login and Security**.
3. Click **Change password**.

4. Enter your current password.
5. Enter your new, complex password or passphrase.
6. Reenter your new password.
7. Click **Require all devices to sign in with new password**.
8. Click **Save**.

If you have inadvertently left yourself logged in to a LinkedIn session elsewhere, checking **Require all devices to sign in with new password** will ensure that all sessions are closed. Further attempts to open LinkedIn from any computer or mobile device will require using the new password.

Two-Step Verification

Two-step verification is an effective means to prevent and identify attempted compromises of your LinkedIn account. Whenever you access your LinkedIn account from a browser that LinkedIn does not recognize, LinkedIn will hold continued access until an unlock code, sent to your mobile phone on file with LinkedIn, is entered. Once the correct unlock code is entered, information that identifies your browser is stored on your computer in the form of a cookie. Afterward, attempts to access your LinkedIn account from that browser, or any authenticated browser for that matter, will require only a username and password. If the cookie is absent or incorrect, you will be challenged once again with a code sent to your mobile phone.

If you no longer have access to the mobile phone required for two step authentication and cannot access your account from an authenticated browser, you will need to contact LinkedIn to enable access.

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 two-step verification.

More importantly, if the person trying to log in to your LinkedIn account has triggered the sending of a verification code then they have entered the correct password for your profile. If you believe this to be the case, you should immediately change your password, follow the steps in **Where You're Signed In** and, if you "recycle" passwords, meaning that you use the same password for other online sites, you should probably change those as well.

To activate **Two-step verification**, from the **Settings & Privacy** menu,

1. Click the **Account** tab.
2. Click **Login and security**.
3. Click **Two-step verification**.
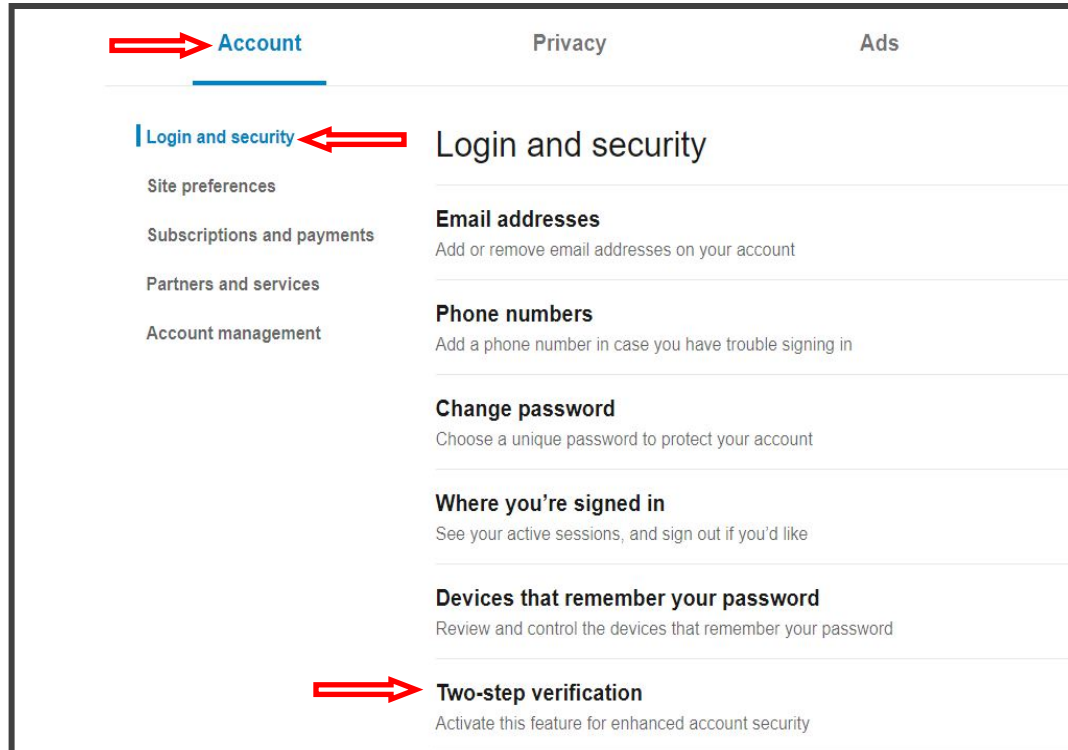
Account | Privacy | Ads

Login and security
Site preferences
Subscriptions and payments
Partners and services
Account management

Login and security

Email addresses
Add or remove email addresses on your account

Phone numbers
Add a phone number in case you have trouble signing in

Change password
Choose a unique password to protect your account

Where you're signed in
See your active sessions, and sign out if you'd like

Devices that remember your password
Review and control the devices that remember your password

Two-step verification
Activate this feature for enhanced account security

Two-step verification
Activate this feature for enhanced account security

Two-step verification is turned off. Turn on

Two step verification gives you additional security by requiring a verification code whenever you sign in on new device. **Learn more**

4. Click **Turn on**.

Two-step verification
Activate this feature for enhanced account security

Choose your verification method

Authenticator App

Cancel   Continue

LinkedIn offers two options for two-step verification: using an authenticator app or mobile telephone. An authenticator app is an additional app–separate from LinkedIn–that generates a random code used to verify your identity when you are logging into a service (e.g., LinkedIn).

To use an authenticator app for two-step verification, install the app of your choice. You will then need to follow steps provided by the authenticator app to add your LinkedIn account to the authenticator app. If you choose this method, codes generated by the authenticator app will be used to sign in to LinkedIn.

To use a mobile telephone number for two-step verification, you will be required to add the number to your account if you have not already done so.

If you have already associated a Mobile number with your account, go to step **14**.

5. Click **Add a phone number**.

Two-step verification
Activate this feature for enhanced account security

Choose your verification method

Phone Number (SMS)

Phone number must be added to activate two-step verification.

Your phone number helps us keep your account secure by adding an additional layer of verification. It also helps others, who already have your phone number, discover and connect with you. You can always decide how you want your phone number used. **Learn more**

Add a phone number

Phone numbers
Add a phone number in case you have trouble signing in

You haven't added any phone numbers yet.

Country

United States

New phone number

8058058056

We'll send a code to this number - you'll need it for the final step.

Cancel   Send code
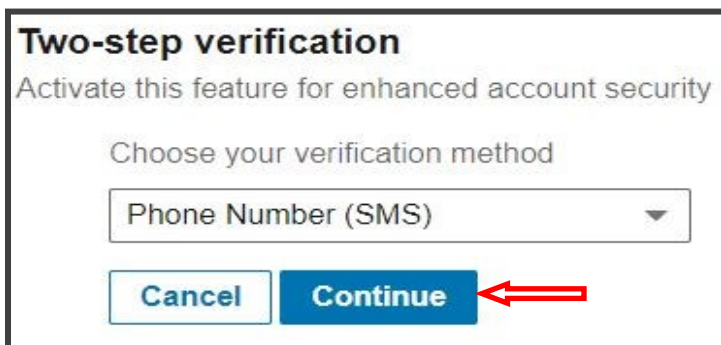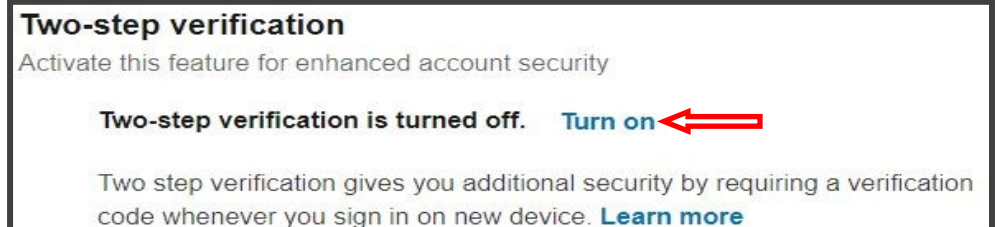
6. Verify the **Country** is set correctly.
7. Enter the mobile telephone number to which you want verification messages sent.
8. Click **Send code**.

9. You will need to add your password to verify the changes made and click **Done**.

For your security, enter your password to make this change

Password

••••••••••••••|

Done ⟵ Forgot password

Phone numbers   Change
Add a phone number in case you have trouble signing in   1 phone number

Phone numbers you've added

US +1 8058058056   Make primary   Remove

☑ Use for password reset
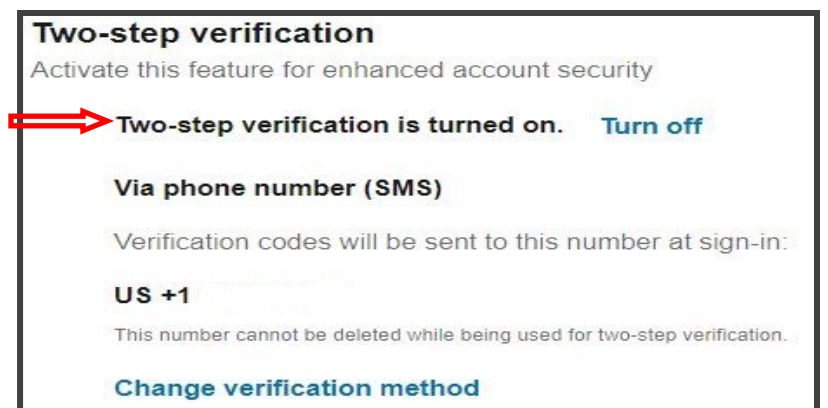
10. Check the mobile telephone for a text message from LinkedIn with the verification code. Enter that code and click **Done**.
11. If all went well, you will see a message showing the telephone number you just added to your account.
12. Return to the **Account** tab and click **Two-step verification**.

Two-step verification
Activate this feature for enhanced account security

Two-step verification is turned off.   Turn on ⟵

Two step verification gives you additional security by requiring a verification code whenever you sign in on new device. **Learn more**

13. Click **Turn on**.

Two-step verification
Activate this feature for enhanced account security

Choose your verification method

Phone Number (SMS)   ▼

Cancel   **Continue** ⟵

14. Choose the verification method and click **Continue**.
15. Enter your password to verify the change and click **Done**.
16. Check the mobile telephone for a text message from LinkedIn with the verification code. Enter that code and click **Done**.

Two-step verification
Activate this feature for enhanced account security

⟹ **Two-step verification is turned on.   Turn off**

Via phone number (SMS)

Verification codes will be sent to this number at sign-in:

US +1

This number cannot be deleted while being used for two-step verification.

Change verification method

17. Next, you will be notified that two-step verification is turned on.

Where You're Signed In

This feature can be used to end any active LinkedIn session. This is more of a security audit tool than a security measure. It will not prevent the compromise of your account but it can tell you if unauthorized access to your account is occurring and may indicate a past compromise if that user did not properly log out. **Where you're signed in** will also help you to identify LinkedIn sessions that you did not properly close.

A generally good security practice is to sign out of any internet activity that requires a login; signing out is a specific menu choice. Closing the browser or restarting the computer without properly logging out may leave open the connection to your LinkedIn session. Then, quite possibly, the next person to open LinkedIn from that computer would have complete access to your LinkedIn profile without being challenged for a password.

Sign Out When You Finish! It is Always a Good Security Practice.
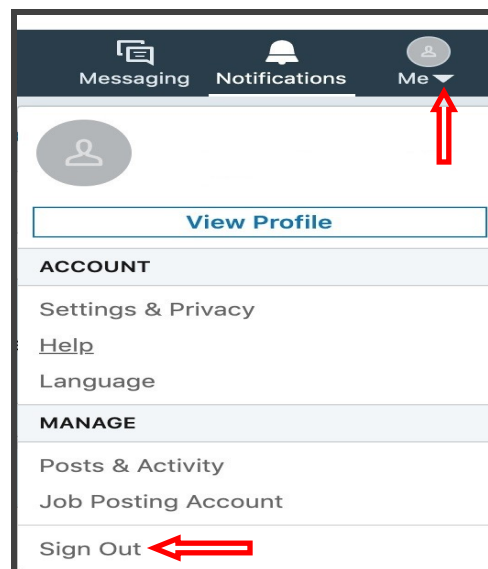
*Click the dropdown arrow next to **Me** and click **Sign Out**.*

To check **Where you're signed in**, from the **Settings & Privacy** menu,

1. Click the **Account** tab.
2. Click **Login and security**.
3. Click **Where you're signed in**.
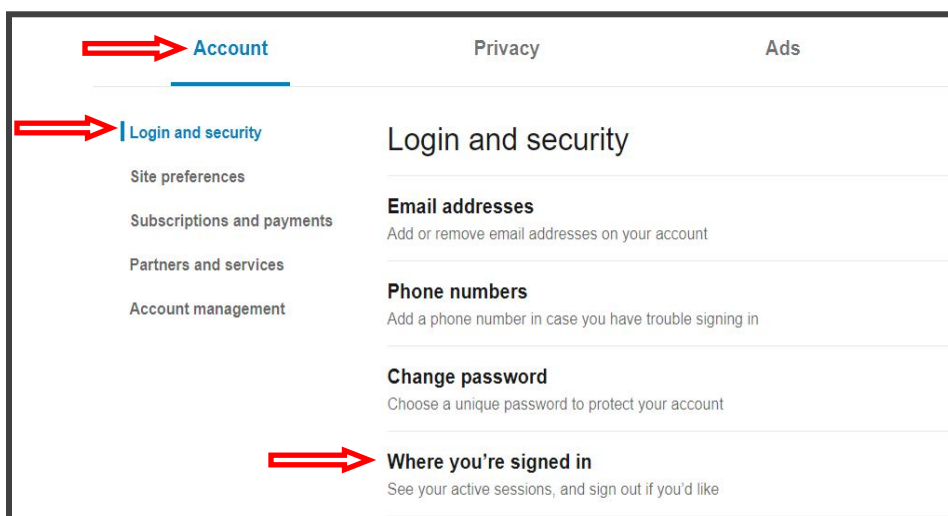
4. Identify session locations that you want to terminate and click **Sign out**. If you find yourself with multiple active sessions, you can terminate them all by clicking **Sign out of all of these sessions**.

5. Enter your password and click **End session**.

Email Address Safety

Email addresses are reliable means to establish connections between individuals. LinkedIn uses email addresses extensively to do so. Even if you have not shared your email address book and none of your business associates have shared their email address book, LinkedIn proposes connections using other and often very effective linking mechanisms.

When selecting an email address to use for LinkedIn, try to separate your professional life from your personal life; avoid using work or official email addresses unless you are representing the organization involved. LinkedIn will use the email address you provide as the primary conduit through which communications flow. LinkedIn will also use your email address to reset your account in the event you are locked out.

Do not enter your email address anywhere other than in a field designated for email addresses. If you include your email anywhere other than in a field labeled specifically for email, it could be indexed by search engines and locatable by anyone on the internet. Also, exposing your email address to the world makes you an easy and attractive target for spam, phishing, spear-phishing, whaling and other types of internet fraud.

The email address you use with LinkedIn will be visible to your 1st degree connections. Therefore, be selective when deciding to accept or reject a connection request. See **Invitations to connect** for more details.

Maintaining Your Email Addresses
LinkedIn requires that at least one email address be associated with each account and LinkedIn prevents any email address being associated with more than one LinkedIn account. LinkedIn allows you to have multiple email addresses associated with your account, but you will be required to designate one as primary.
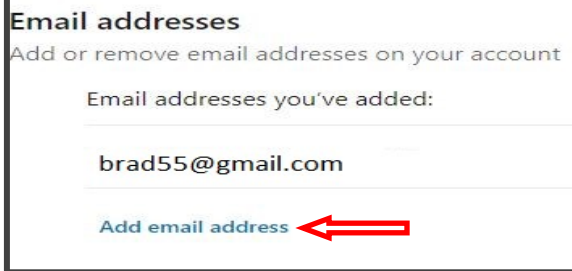
Linking multiple email addresses to your LinkedIn account is a good idea. It allows you multiple avenues of account recovery if you lose access to your primary email account. This could happen if you use a work email address and change jobs or if your employer changes email access policies. It could also happen if your email address is from your ISP and you change ISP without first updating your LinkedIn account.

You can delete any associated email address except your primary email address. In order to delete your primary address, you must first add and then designate as primary a new address. Whenever you add a new email address, LinkedIn sends a verification email to it. The final connection to your profile happens when you confirm the email address by clicking the emailed link.

To add, change, or delete an associated email address, from the **Settings & Privacy** menu,

1. Click **Account**.
2. Click **Login and security**.
3. Click **Email addresses**.
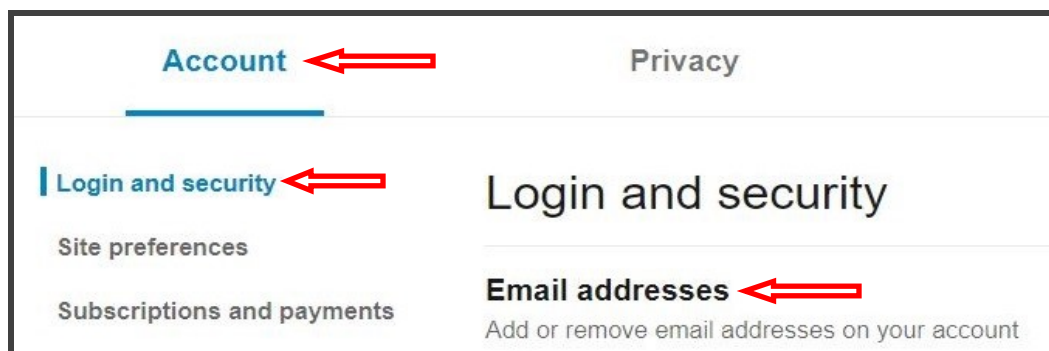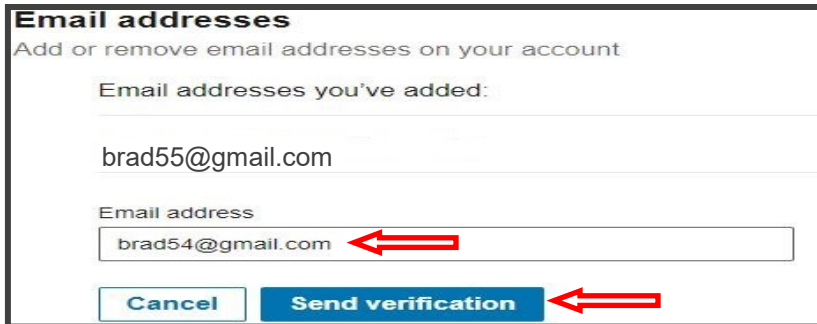
4. Click **Add email address**.

5. Enter the new address and click **Send verification**.
6. Check the new email's inbox for a LinkedIn email and follow the instructions there to activate the new email address.

Sharing Your Address Books
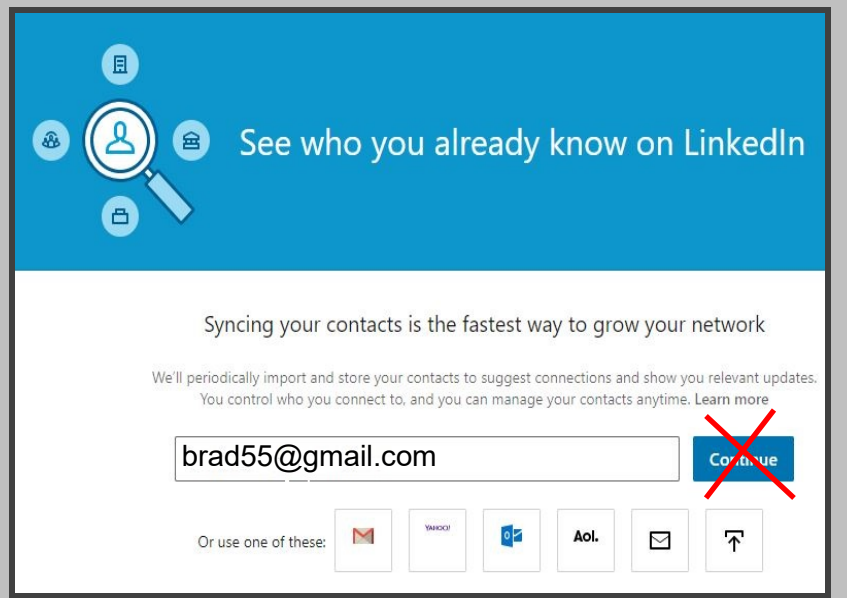
Automatically adding contacts from your email address books is one way LinkedIn helps you build your network. Superficially, quickly building your network by sharing your address book seems to be a good thing. After all, that is why you are on LinkedIn. However, in order to add contacts from your email address books, you will be required to provide LinkedIn with the password to your email account.

As trustworthy as LinkedIn is, providing any-one with any of your passwords is contrary to just about every recommended computer se-curity practice. And, allowing a third party site to access a work email address book may violate company policies and perhaps even employment agreements.

Before allowing a third party site, like LinkedIn, access to your address books, ask yourself if you would appreciate someone exposing your name and email address to a site you did not choose. Moreover, consider whether or not you want to be professionally associated with everyone in your address book.

As you use LinkedIn, you will be presented with many opportunities to expand your network. Some opportunities will appear with names and brief biographies of people LinkedIn believes you are associated with.

LinkedIn allows you to sync your contacts for networking opportunities; however, it is not mandatory. Opting out ensures the privacy of your contacts and it is not the only way to make connections. LinkedIn, using matching algo-rithms, will present you with potential connections to individuals whom already have LinkedIn profiles.

The notices allow easy one-click ways to make connections. Most will be people you know–on some level. (LinkedIn's matching algorithms are very effective–it is their stock-in-trade.) Some people you will not know. But knowing someone and connecting with them in a professional sense are different things. Choose wisely before you accept just anybody's connection request. (See **Invitations from your network**.)

Profile Settings

Your profile says everything about you. It is your LinkedIn presence. Take care with what you post and remember that first impressions are everything.

Controlling Who Can See Your Connections

If you have properly managed your connections (you will find more information about managing connections in the **Invitations from your network** section), then your list of connections says an awfully lot about who you are. That list also contains information that can be exploited by someone with a mind to do so. By default, 1st and 2nd level connections can see your entire connections list.

Restricting access to your list of connections is a good practice. Be mindful, however, that even at the most restrictive setting your 1st degree connections will always be able to see mutual connections.

To change **Who can see your connections**, from the **Settings & Privacy** menu,

1. Click the **Privacy** tab.
2. Click **How others see your profile and network information**.
3. Click **Who can see your connections**.
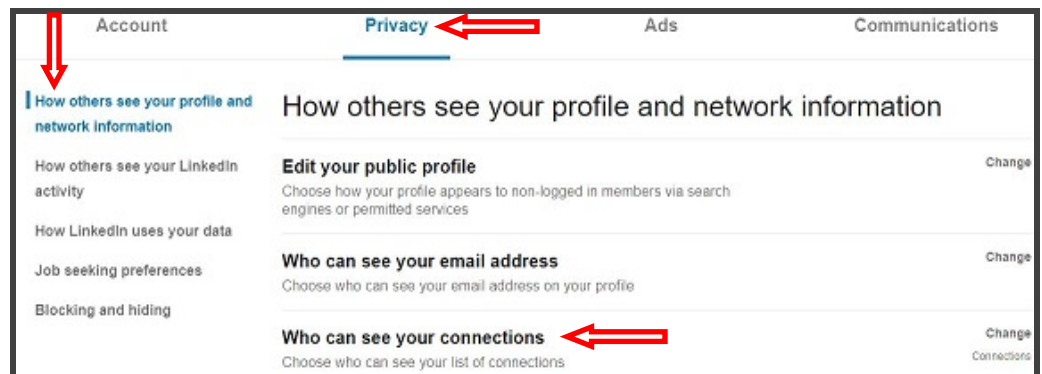
4. If **Only you** is your current setting, you need do nothing more. Otherwise,
5. Click the **Down arrow**.
6. Click **Only you**.
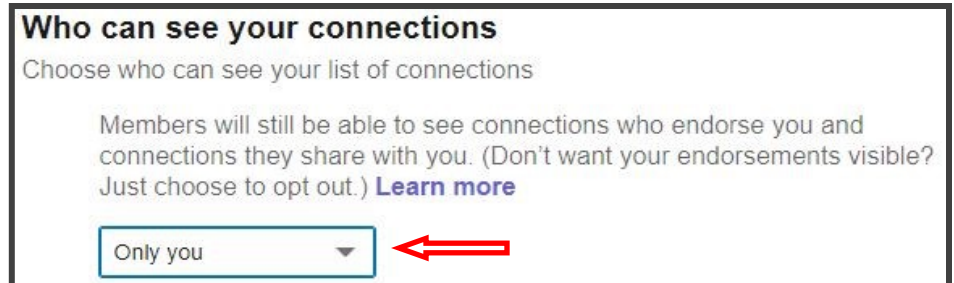
Limit Public Access to Your Profile

When you restrict access to your LinkedIn profile to only logged in LinkedIn members, you not only reduce your identity theft vulnerability, you also prevent it being indexed by search engines.

The most restrictive setting is **Make my public profile visible to no one**. With this setting, your profile will still be visible to logged in LinkedIn members: Your profile will not be available to nonmembers, members not logged in and search engines such as Google, Yahoo, Bing, etc.

When deciding upon a setting, consider why you are on LinkedIn. Perhaps you do want people to locate your profile using an internet search site. Perhaps you do not. Perhaps you want your profile to be viewable to people who are not LinkedIn members. Perhaps you do not.

Generally speaking, a recruiter or company seeking candidates will not browse anonymously or without having logged in to LinkedIn. Nor would a recruiter rely on internet search engines to identify suitable candidates. Therefore, changing **your profile's public visibility** is probably a good choice.

To limit who has access to your public profile, from the **Settings & Privacy** menu,

1. Click the **Privacy** tab.
2. Click **How others see your profile and network information**.
3. Click **Edit your public profile**.
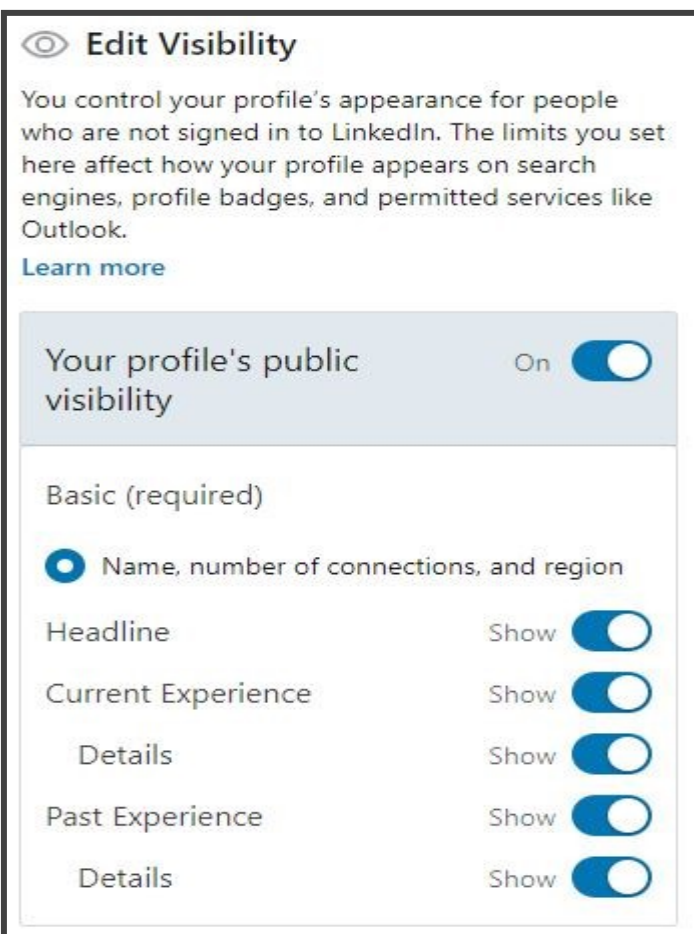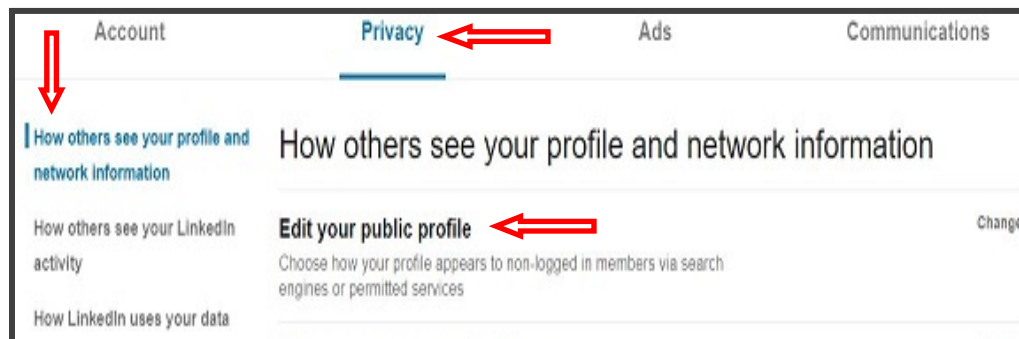
4. In **Edit Visibility**, select the setting you feel most comfortable with.

* If you feel compelled to keep your profile visible to everyone, consider restricting other information that could increase your risk for identity theft and phishing. **Information already indexed by search engines will persist for an unknown period of time.**

Controlling What Others See When You View Their Profile

Consider how much information you want others to know about you when you view their profile or when you view their company profile. Less is probably better. If you are viewing profiles and want the profile owner to know that you are, then sending a LinkedIn InMail message is probably more effective.

Regardless of this setting, your full name and profile image will be visible whenever you browse the profile of one of your 1st level connections.

If you choose **Private profile characteristics**, when you browse a connection other than one of your 1st level connections, the only information they will be able to see is a description of your title and industry and your location. Your name will not appear.

If you choose **Anonymous LinkedIn Member** and browse someone else's profile, that profile owner will not know. The downside? If you have a basic (free) account and choose to browse anonymously, you will be unable to see the list of members that have viewed your profile. When deciding between **Private profile characteristics** and **Private mode**, consider why you are using LinkedIn and how publicly available you want your information and activities to be.

To change how others see your profile when you browse their profiles, from the **Settings & Privacy** menu,
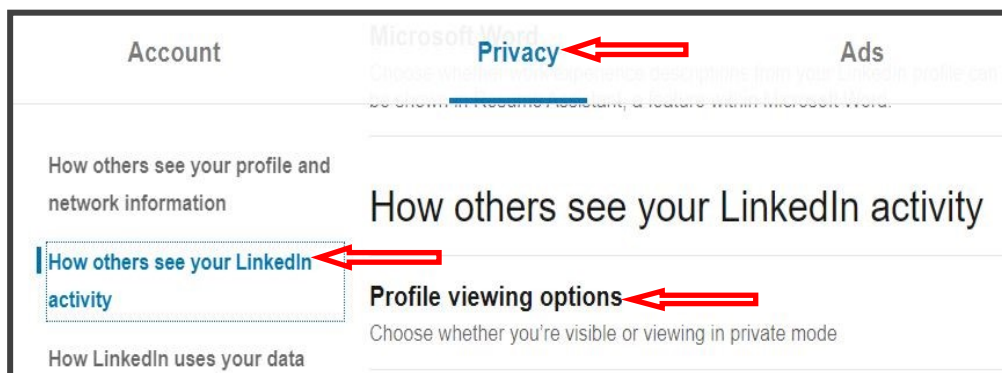
1. Click the **Privacy** tab.
2. Click **How others see your LinkedIn activity**.
3. Click **Profile viewing options**.

4. At a minimum, change the setting to **Private profile characteristics**.
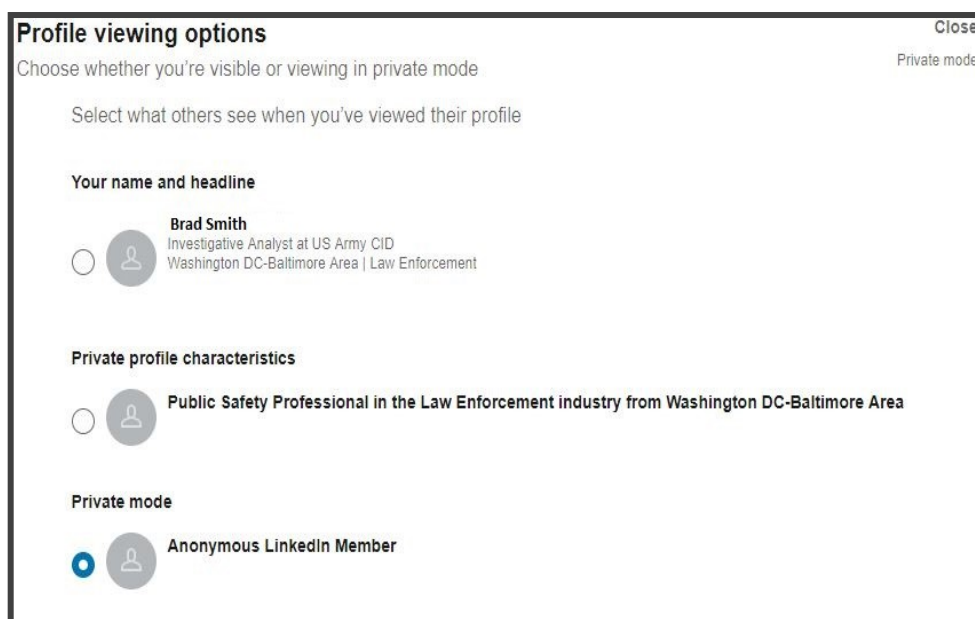
Managing Connections

Removing a Connection, and Blocking or Reporting a LinkedIn Member

You can remove an existing connection, selectively block any LinkedIn member from viewing your profile or you can report any LinkedIn member for a number of different inappropriate behaviors. If you remove, block or report a user, LinkedIn will not notify that member. If you are connected and block or report that individual then that connection will be removed. If either has endorsed the other, then those endorsements will be deleted and neither will be able to view the other's profile or exchange LinkedIn messages.

Be aware, you cannot block anyone from information you have on your public profile or from information you have posted in open groups. Nor can you block a member from commenting on any post you have made in a public discussion group. Mutual connections can share your information with members whom you have blocked.

To manage your connections,

1. Click **My Network** in the command ribbon across the top of the home page.
2. Scroll down to the **Manage my network** menu and click on **Connections**.
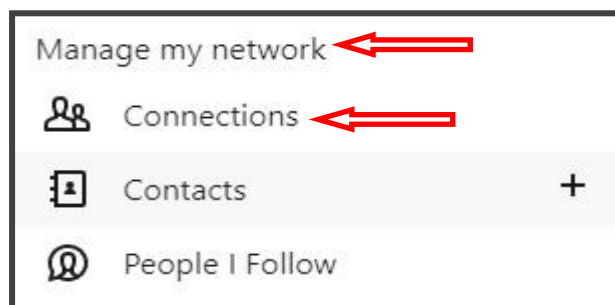
3. Scroll down to the profile name of the person you want to block or do a by name search. Click on the person's name or photo.
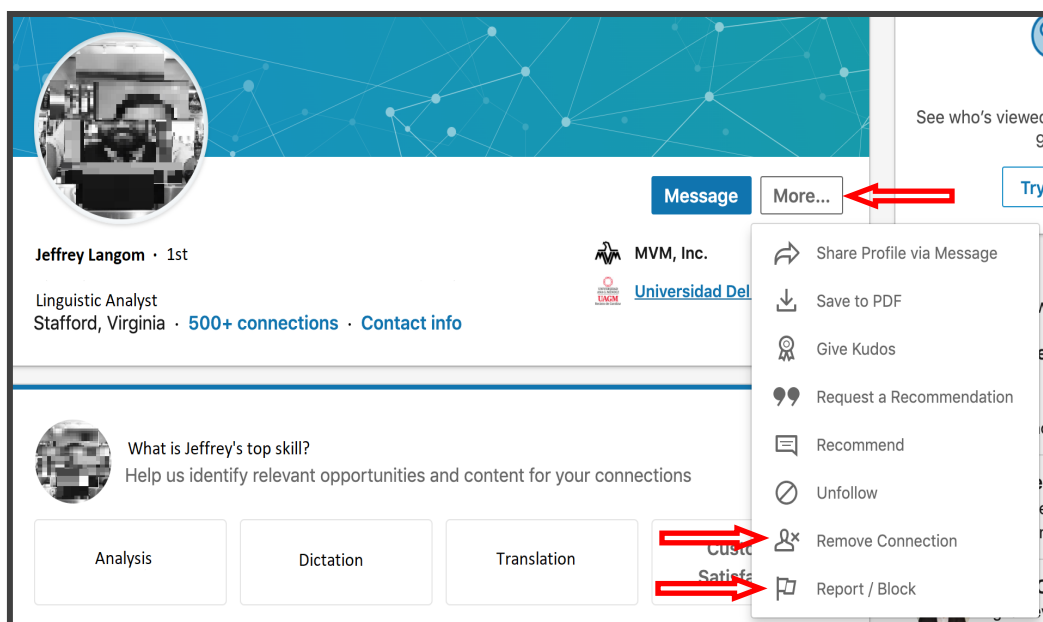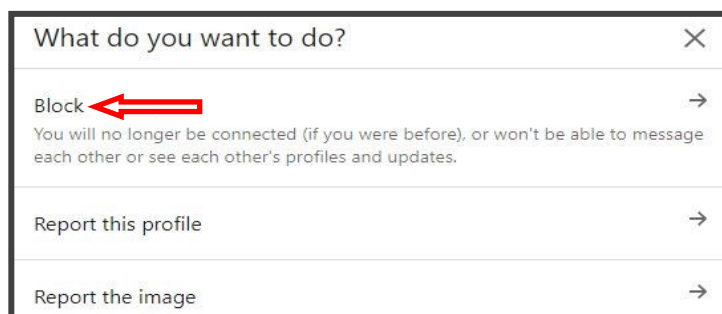
4. Click **More**.
5. Click **Remove Connection** or **Report/Block** depending upon your purpose.

If you choose to remove the connection, you will now see the wording **Connection Removed** in the **More** menu.

If you want to block the connection,
1.   Click anywhere in the row labeled **Block**.

What do you want to do?   ✕

Block   →
You will no longer be connected (if you were before), or won't be able to message each other or see each other's profiles and updates.

Report this profile   →

Report the image   →

2.   Read LinkedIn's explanation of the changes you are about to make. If you agree, click **Block**.
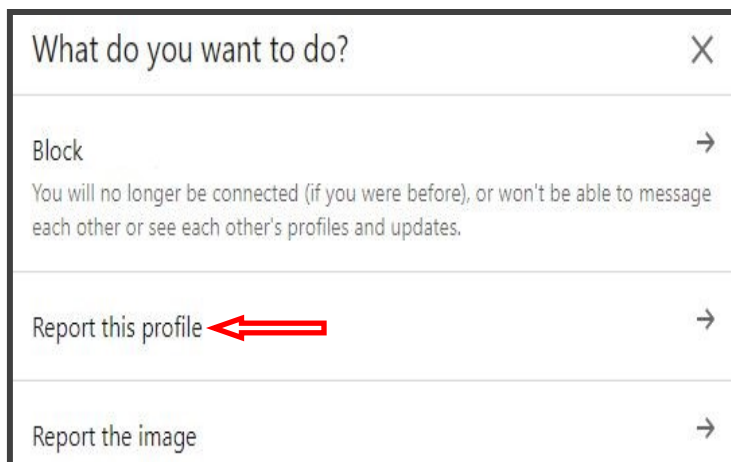
Are you sure you want to block Jeffrey?   ✕

You will no longer be connected (if you were before), or have endorsements and recommendations from this person.
You will also no longer see any suggestions to interact with each other.

Go back   Block

LinkedIn gives you the opportunity to report someone's profile or just their image. If you want to report the profile,
1.   Click anywhere in the row labeled **Report this profile**.
2.   There are ten reasons provided for reporting a profile. Select one.
3.   Click **Submit**.
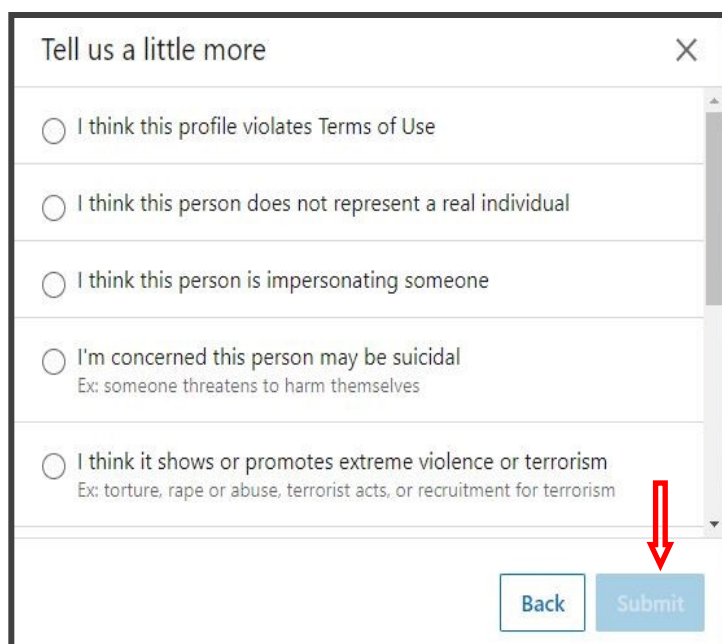
What do you want to do?   ✕

Block   →
You will no longer be connected (if you were before), or won't be able to message each other or see each other's profiles and updates.

Report this profile   →

Report the image   →

Tell us a little more   ✕

○ I think this profile violates Terms of Use

○ I think this person does not represent a real individual

○ I think this person is impersonating someone
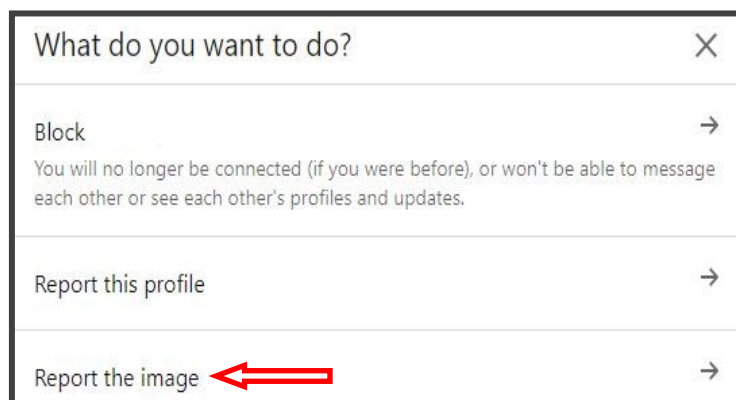
○ I'm concerned this person may be suicidal
Ex: someone threatens to harm themselves

○ I think it shows or promotes extreme violence or terrorism
Ex: torture, rape or abuse, terrorist acts, or recruitment for terrorism

Back   Submit
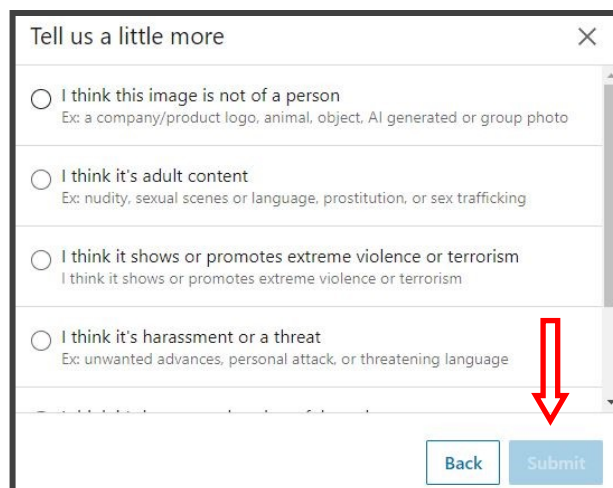
If you want to report the image,

1. Click anywhere in the row labeled **Report the image**.
2. There are six reasons provided for reporting the image. Select one.
3. Click **Submit**.

What do you want to do?

Block
You will no longer be connected (if you were before), or won't be able to message each other or see each other's profiles and updates.

Report this profile

Report the image
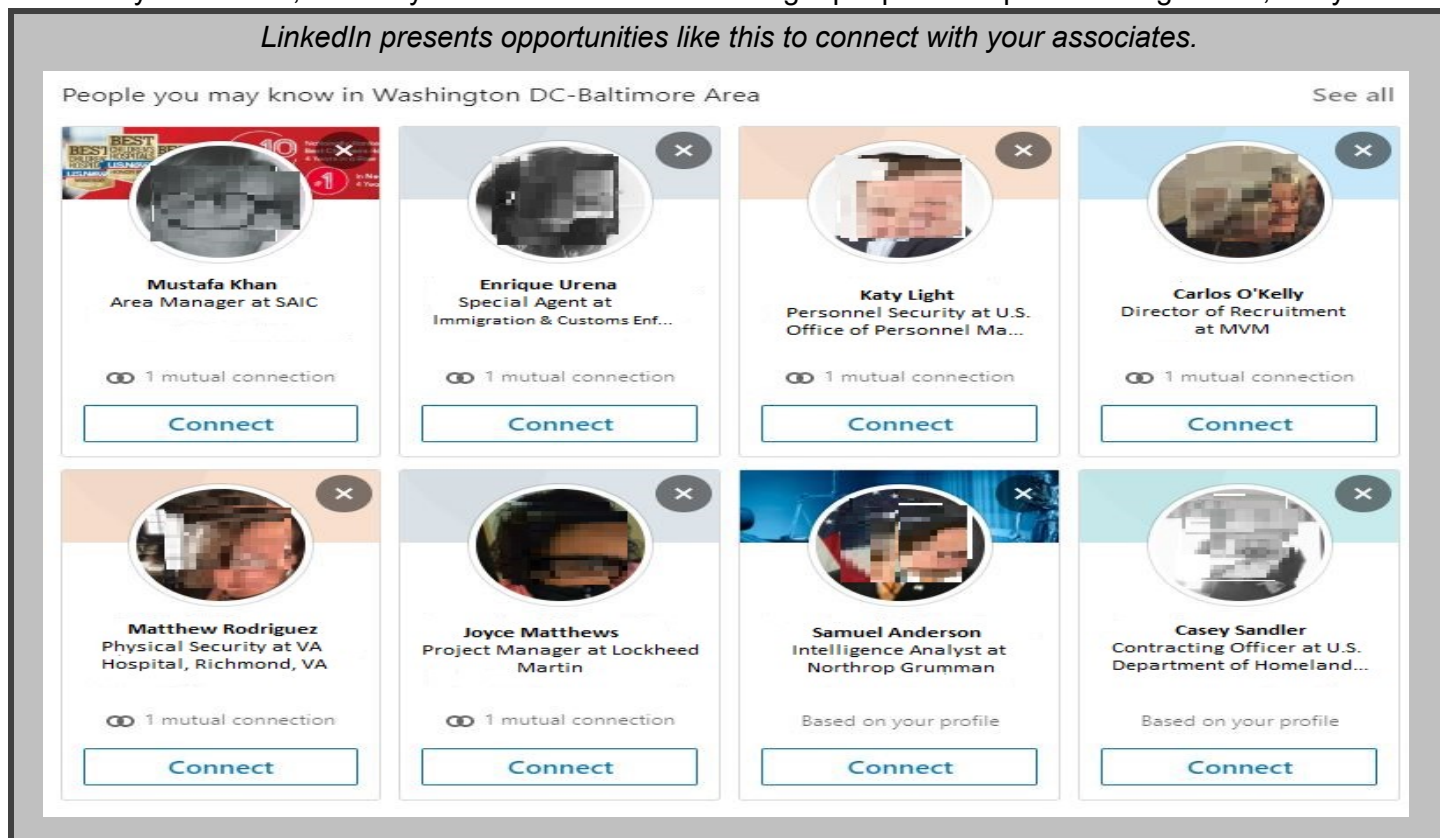
Tell us a little more

○ I think this image is not of a person
Ex: a company/product logo, animal, object, AI generated or group photo

○ I think it's adult content
Ex: nudity, sexual scenes or language, prostitution, or sex trafficking

○ I think it shows or promotes extreme violence or terrorism
I think it shows or promotes extreme violence or terrorism

○ I think it's harassment or a threat
Ex: unwanted advances, personal attack, or threatening language

Back   Submit

Requesting a Connection

Finding connections is easy because LinkedIn employs multiple means to locate people and, often without effort on your part, suggests connections. This is important to know because it shows how easily others, including untrustworthy individuals, with only minimal information can target people with specific backgrounds, like you.

LinkedIn presents opportunities like this to connect with your associates.

People you may know in Washington DC-Baltimore Area   See all

Mustafa Khan
Area Manager at SAIC
1 mutual connection
Connect

Enrique Urena
Special Agent at Immigration & Customs Enf...
1 mutual connection
Connect

Katy Light
Personnel Security at U.S. Office of Personnel Ma...
1 mutual connection
Connect

Carlos O'Kelly
Director of Recruitment at MVM
1 mutual connection
Connect

Matthew Rodriguez
Physical Security at VA Hospital, Richmond, VA
1 mutual connection
Connect

Joyce Matthews
Project Manager at Lockheed Martin
1 mutual connection
Connect

Samuel Anderson
Intelligence Analyst at Northrop Grumman
Based on your profile
Connect

Casey Sandler
Contracting Officer at U.S. Department of Homeland...
Based on your profile
Connect
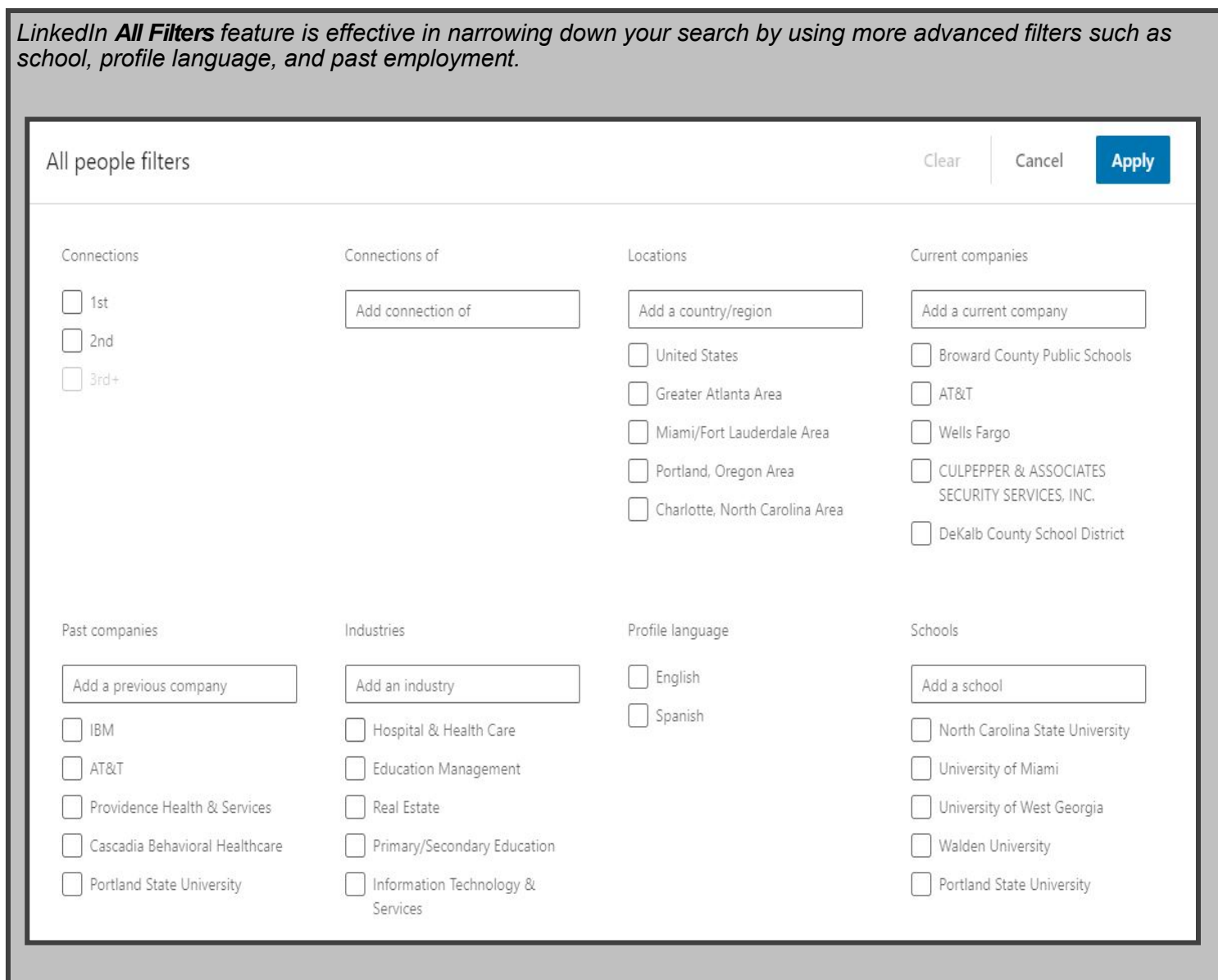
For a more specific search, or if you want to search for someone with a special or unique background, the **Connections**, **Locations**, and **Current companies** filters can be very affective. For an even more in depth search, you should select **All Filters**.

*LinkedIn **All Filters** feature is effective in narrowing down your search by using more advanced filters such as school, profile language, and past employment.*

*Choosing **All Filters** provides additional search capabilities.*

Contact interests

☐ Probono consulting and volunteering

☐ Joining a nonprofit board

Services

Add a service category

☐ Commercial Real Estate

☐ Real Estate

☐ Property Management

☐ Mortgage Lending

☐ Relocation

First name

Last name

Title

Company

School

Accepting Connection Requests

When someone attempts to connect with you, a small number appears on the **Home**, **My Network**, and **Notifications** icons on the command ribbon. To accept or reject the connection requests,

1. Click **Home**, **My Network**, or **Notifications**.

Home   My Network   Jobs   Messaging   Notifications   Me ▼

Jeffrey invited you to connect

Jeffrey Langom
Linguistic Analyst
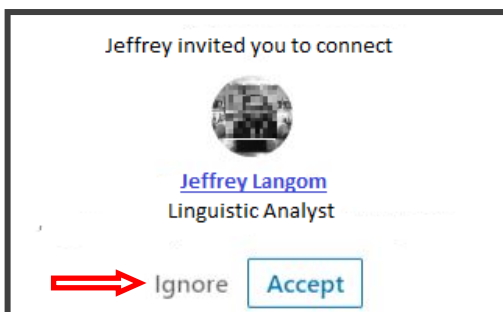
Ignore   Accept

2. If you click **Home** or **Notifications**, you will see a message at the top of your screen with the image, name, and professional title of the person requesting to connect. Click **Ignore** or **Accept**.

Invitations   Manage

Jeffrey Langom
Linguistic Analyst
                    Ignore   Accept

3. If you click **My Network**, you will see a message in the middle of your screen with the image, name, and professional title of the person requesting to connect. Click **Ignore** or **Accept**.

Endorsements and Recommendations

Endorsements recognize an individual's skills and abilities, are generalized in nature, and require very little interaction to create. Recommendations, the digital equivalent of a Letter of Recommendation, are more specific and require that the recommender write particulars. Both are visible to connections and the public if you have not secured your profile. (See **Limit Public Access to Your Profile**).

If you have been endorsed for knowledge, skills and abilities that you do not have or if you no longer want an endorsement from a specific individual or for a specific skill, you can delete the endorsement. Your endorser will not be notified of your decision to delete the endorsement. You can also delete endorsements you have mistakenly given to others. Be careful about accepting recommendations. You cannot delete a recommendation. You can only hide it from your profile.

Removing Endorsements from Your Profile
If someone has endorsed you for a skill you do not have or for a skill you do have but would prefer not to broadcast, you can delete that entire skill category.
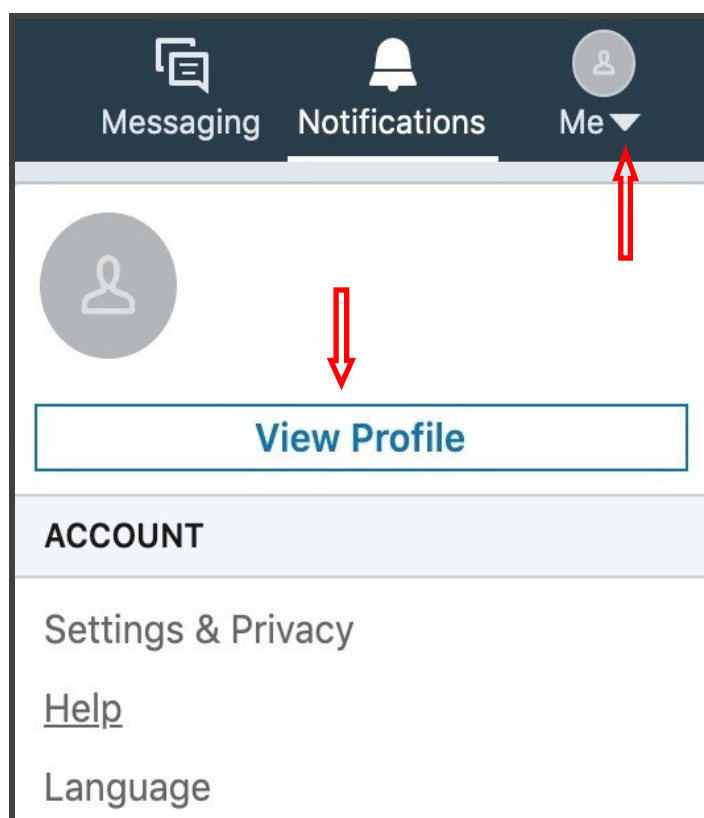
1. In the command ribbon, click the down arrow next to **Me**.
2. Click **View Profile**.

3. Scroll down your profile until you see the **Skills & Endorsements** section.
4. Click the **pencil** icon to edit the section.
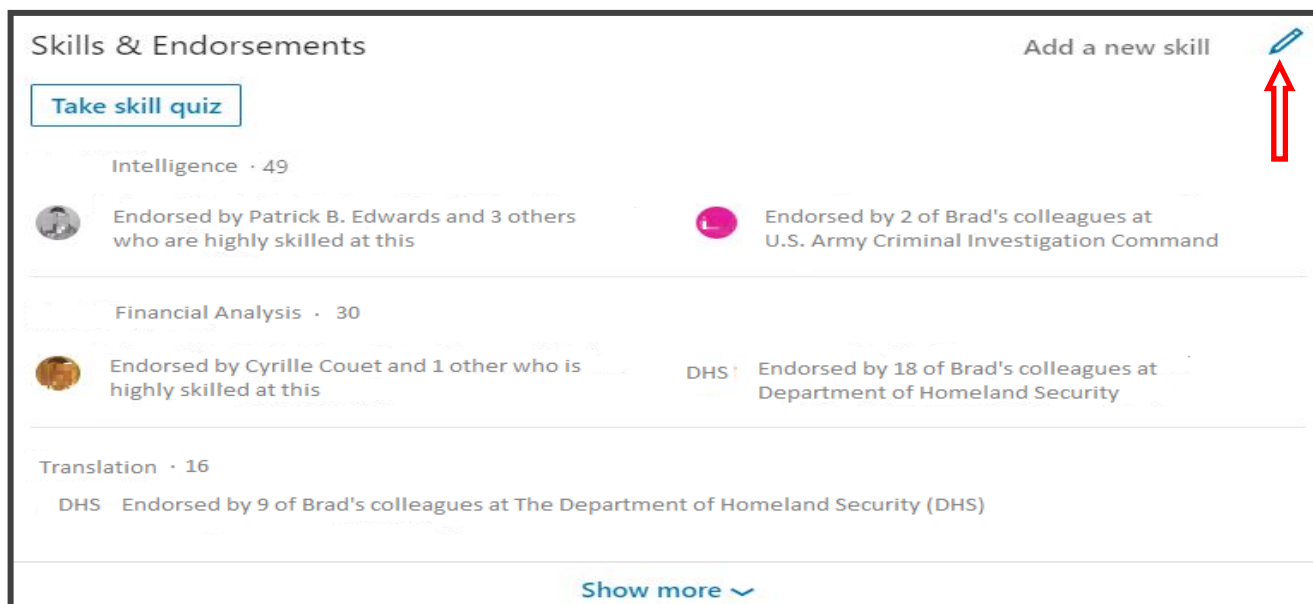
5. Opposite each of the skills is a trash can icon. Click on the trash can icon opposite the skill you wish to delete.
6. Click **Save**.
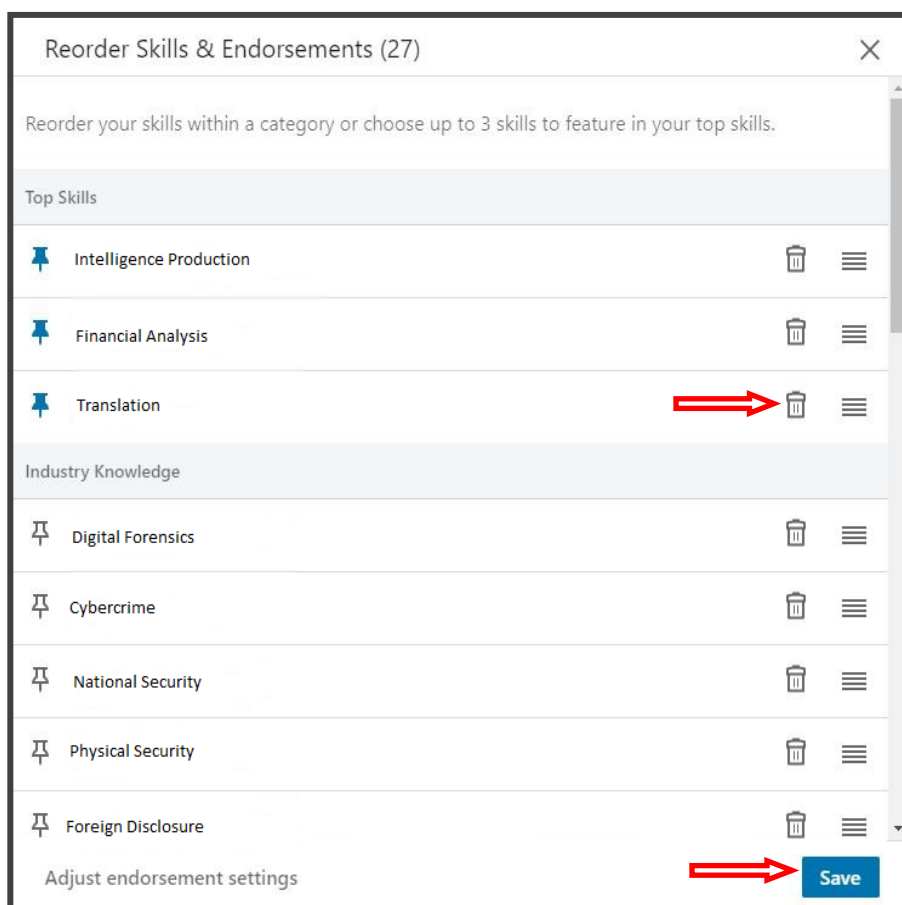
Hiding an Individual's Endorsement of You

If you find that you have been endorsed by someone and no longer want that endorsement, you can hide that connection's endorsement without deleting the entire skill category.

Hiding a connection's endorsement for a specific skill does not delete all endorsements from that person. If you feel you need to delete multiple endorsements from a connection, then perhaps it is time to reevaluate the relationship you have with that LinkedIn connection. Deleting a connection also deletes any endorsements they might have given you. The individual will not be notified if you break the connection.

To hide an endorsement, from the **View Profile** page,

1. Scroll down your profile to the **Skills & Endorsements** section.
2. Click on particular skill for the endorsement you want to hide.
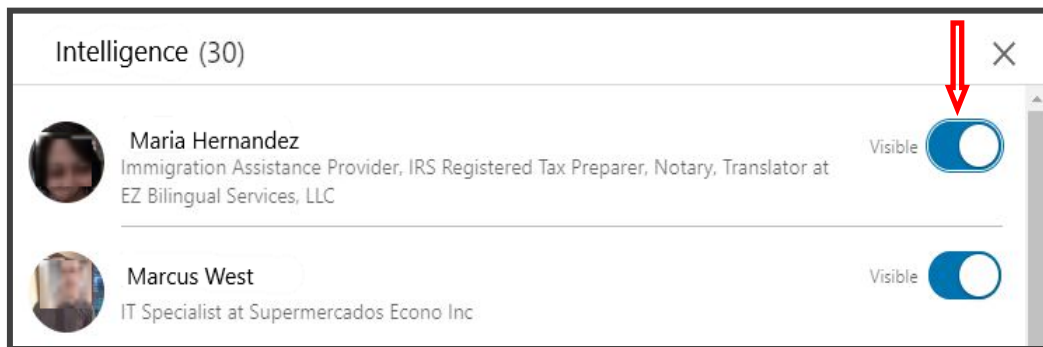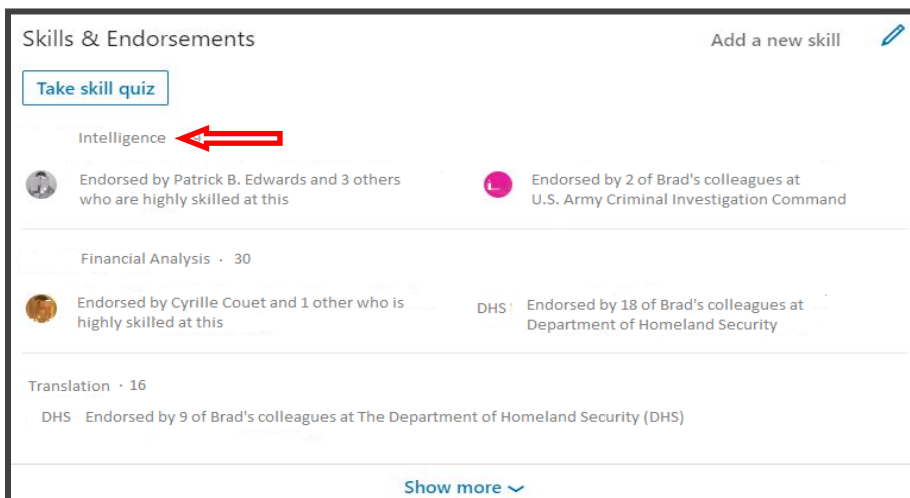
3. Scroll to the name of the connection whose endorsement you wish to hide.
4. Click on the toggle opposite the connection.

The wording next to the toggle will change from "Visible" to "Hidden."
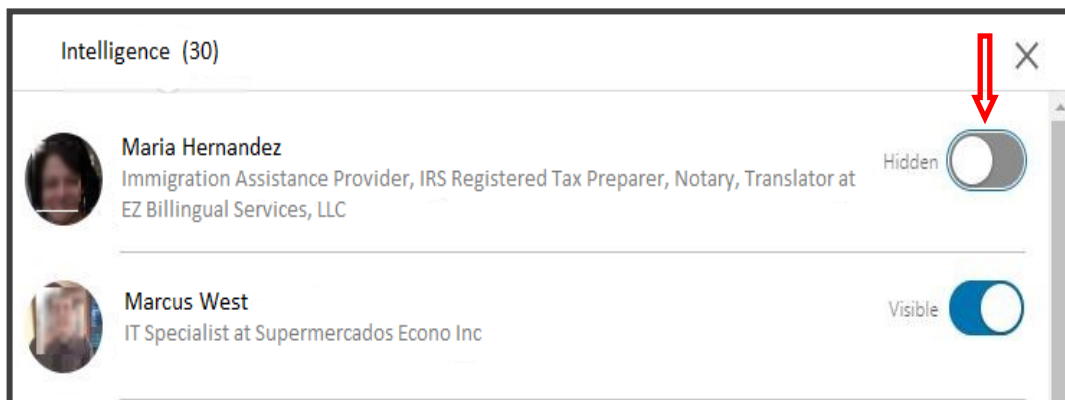
Removing Endorsement You Have Mistakenly Made

If you find that you have endorsed someone for a skill they do not have or for a skill you no longer want to endorse them for, you can delete that endorsement. Your connection is not notified that you have deleted the endorsement.

To remove an endorsement you have mistakenly made,

1. Navigate to that person's LinkedIn profile page and scroll down to the **Skills & Endorsements** Section.
2. Skills that you have endorsed are represented by a check mark. Click on the check mark to reverse your endorsement.

The check mark will revert to a plus sign (+) and your endorsement for that skill will be gone from the person's profile.
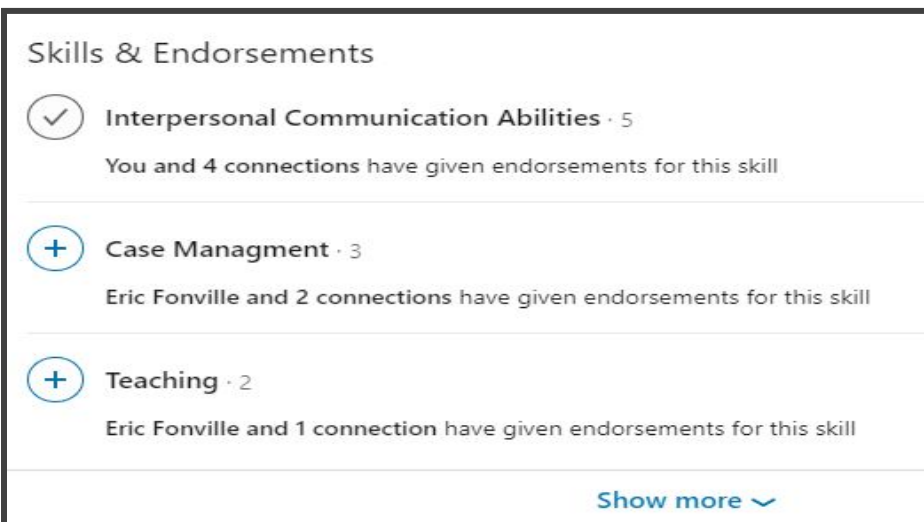
Hiding Recommendations on Your Profile

Recommendations appear in your profile beneath **Skills & Endorsements** and are accessed by editing your profile. You cannot delete a recommendation once you have accepted it to your profile. You can only hide it from view.

To hide an endorsement,

1. In the command ribbon, click the drop down arrow next to **Me**.
2. Click **View Profile**.
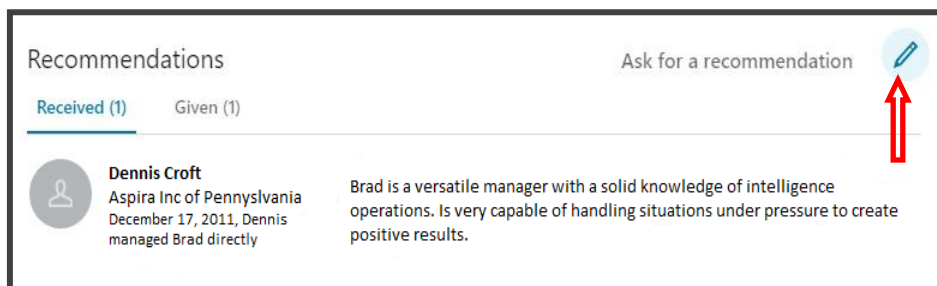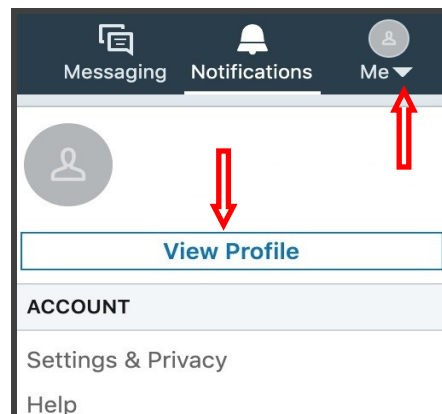
3. Scroll down to the **Recommendations** section.
4. Click the pencil icon to edit your recommendations.
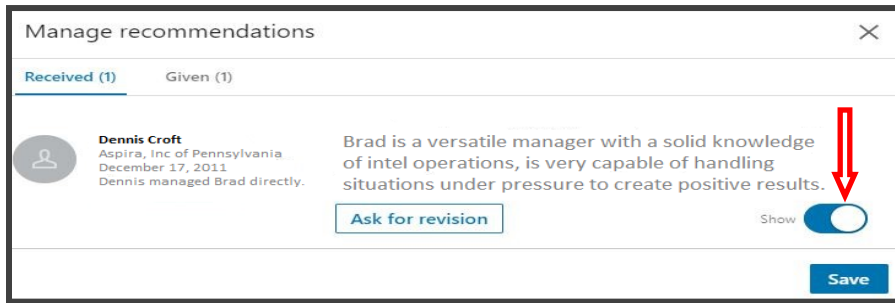
5. Click the toggle located next to the recommendation you wish to hide.

The wording next to the toggle will change from "Show" to "Hide."

6. Click **Save**.
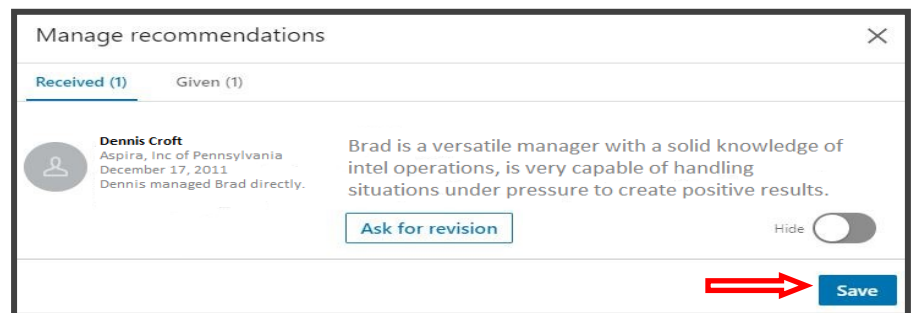
Downloading an Archive of Your LinkedIn Activity

You might find yourself in a situation where you would like to review all of your LinkedIn activity. Fortunately, there is a means by which you can accomplish this without scrolling through innumerable LinkedIn pages. You can download to your local computer an archive of your information and activity.

Actually, you have options for downloading your data. You can select among eight data files to download particular information which will be ready within 10 minutes or you can choose to download a larger, more in-depth data archive. The larger archive includes information such as connections, account history, as well as information LinkedIn infers about you based on your profile and activity.

DO NOT download an archive of your LinkedIn data to any computer that you do not have total ownership of. Do not download an archive to a borrowed computer, a public computer like those you might use at a library, community center or school, or your work computer.

To download an archive of your LinkedIn activity, from the **Settings & Privacy** menu,

1. Click the **Privacy** tab.
2. Click **How LinkedIn uses your data**.
3. Click **Get a copy of your data**.
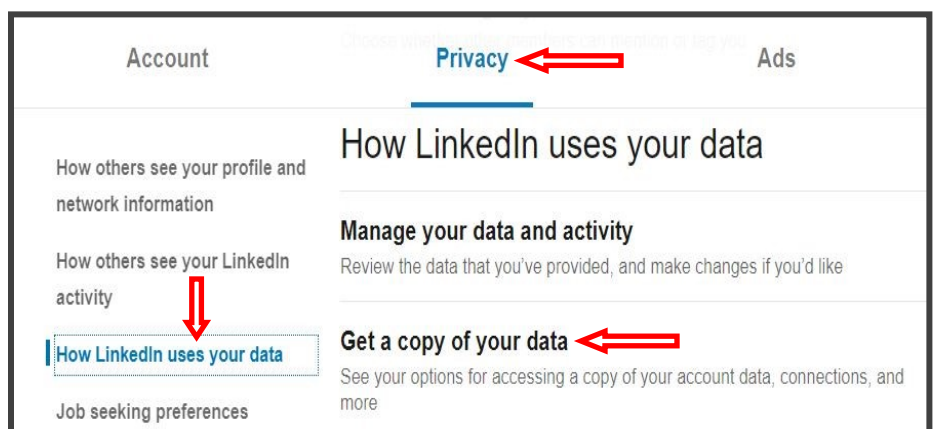
4. If you wish to receive a condensed archive of your LinkedIn data, select the radial next to **Want something in particular**?
5. Choose the particular data files you are interested in.
6. Click **Request archive**. You will be asked to enter your password to verify the request.

7. Periodically check the inbox of the email address associated with your LinkedIn account. Look for a message indicating your data is available for download.
8. Click the **download your data archive using this link** featured in the email. You will be redirected to LinkedIn.
9. Click **Download archive**.

To obtain a more in-depth archive,

1. Click the radial next to **Download larger data archive**.
2. Click **Request archive**.
3. Similar to obtaining a condensed archive, you will have to monitor your email inbox for the message indicating your archive is available.
4. Click the link in the email or navigate to LinkedIn to download the archive.

Remember. Obtaining the larger archive may take up to 24 hours.

For further assistance, see **LinkedIn Help**.

The Army's Digital Detectives