



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

Phone: 571.305.4482 IDSN 2401
Fax: 571.305.4189 IDSN 2401

Email CCIU

CCIU Webpage



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



"DO WHAT HAS TO BE DONE"

CPF 00004-16-CID361-9H-LinkedIn*

19 September 2016

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. LinkedIn is not for staying in touch with family members, fraternity and sorority brothers and sisters, former roommates or childhood friends. 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 don't 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 on LinkedIn. 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 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

* This LinkedIn configuration guide supersedes CID Crime Prevention Flyer CPF-00009-15-CID361-9H.

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:

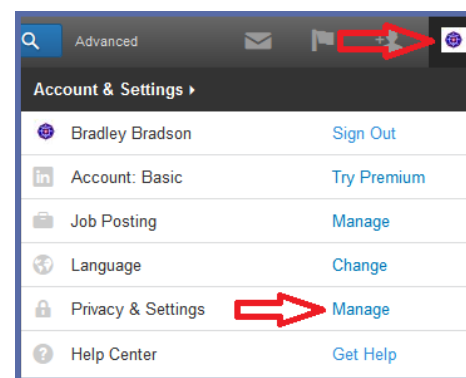
- Do not include in your profile that you have a security clearance.
- Exercise appropriate skepticism when contacted by someone not known to you regardless of how credible their LinkedIn presence appears. Not everyone on the internet is who they say they are.
- Be cautious when considering a connection request from those you do not know.
- 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.

Privacy and Settings

To access **Privacy and Settings**, hover your mouse above your profile picture in the upper right of your LinkedIn home page. When the **Accounts & Settings** menu appears, click **Manage**.



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. 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 are more likely to survive a [dictionary attack](#) than is a single word.

Changing passwords is a straightforward process. A good security 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 **Privacy and Settings** menu,

The screenshot shows the LinkedIn 'Account' settings page. At the top, there are two tabs: 'Account' and 'Privacy'. A red arrow points to the 'Account' tab. Below the tabs, there are several sections: 'Basics', 'Third parties', 'Subscriptions', 'Email addresses', 'Phone numbers', and 'Change password'. A red arrow points to the 'Basics' section. Under the 'Basics' section, there is a red arrow pointing to the 'Change password' option, which is described as 'Choose a unique password to protect your account'.

1. Click the **Account** tab.
2. Click **Basics**.
3. Click **Change password**.

4. Enter your current password.
5. Enter your new, complex password or passphrase.
6. Reenter your new password.
7. Click **Sign out of all sessions**.
8. Click **Save**.

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

The screenshot shows the 'Change password' form. It starts with the title 'Change password' and a subtitle 'Choose a unique password to protect your account'. Below this, it says 'Passwords are case-sensitive and must be at least 6 characters.' There are three input fields: 'Type your current password', 'Type your new password', and 'Retype your new password'. Red arrows point to each of these fields. Below the input fields, there is a checkbox labeled 'Sign out of all sessions?' with a red arrow pointing to it. At the bottom, there is a blue 'Save' button with a red arrow pointing to it.

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, 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 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**.

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.

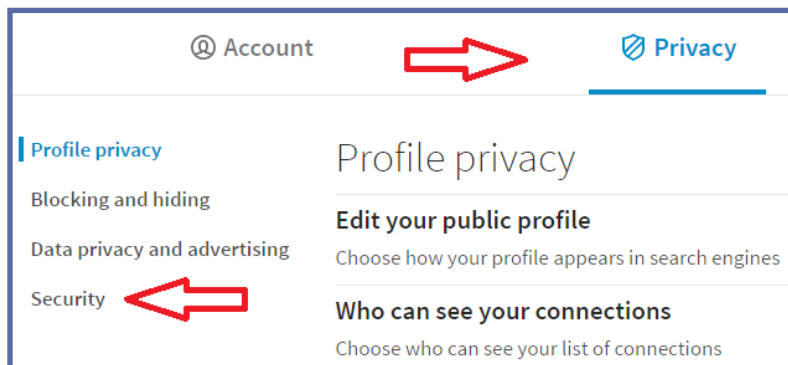
If you, or anyone for that matter, try to login to your LinkedIn account from an unverified browser or if the cookies associated with an authorized browser are deleted, a verification code will be sent as a text message to the mobile phone of record and you will be required to enter that verification code before you will be allowed to access your account.

The defensive benefit of **two-step verification** is the text message you receive notifying you of access from a not yet authorized browser. If you receive a login notification and are not trying to log in, then someone unknown to you is trying to access your LinkedIn account.

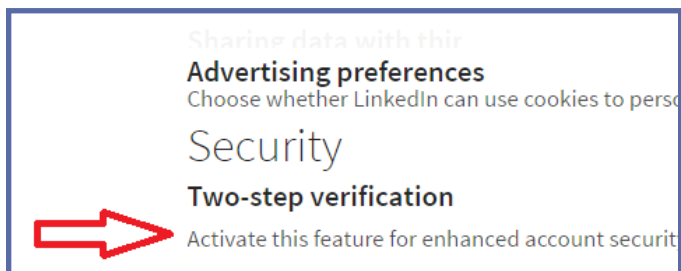
More importantly, if the person trying to log in to your LinkedIn account has triggered the sending of a verification code then they have entered the correct password for your profile. If you believe this to be the case, you should immediately change your password, follow the steps in **See Where You're 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 **Privacy and Settings** menu,

1. Click the **Privacy** tab.
2. Click **Security**.

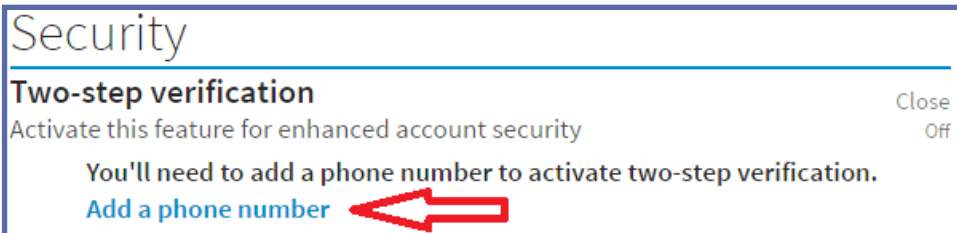


3. Click **Two-step verification**.



4. You will be required to add a mobile phone number to your account if you've not already done so.

If you have already associated a mobile number with your account, go to step 11.



Security

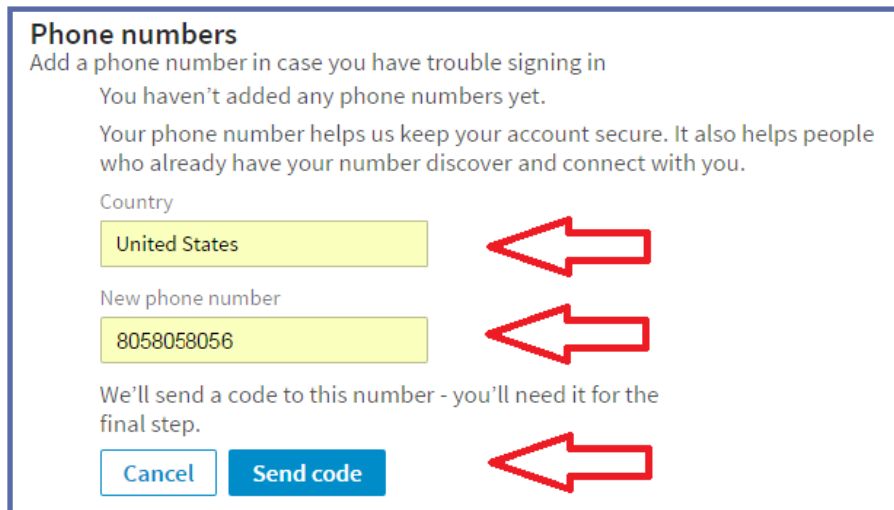
Two-step verification

Activate this feature for enhanced account security

You'll need to add a phone number to activate two-step verification.

[Add a phone number](#)

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



Phone numbers

Add a phone number in case you have trouble signing in

You haven't added any phone numbers yet.

Your phone number helps us keep your account secure. It also helps people who already have your number discover and connect with you.

Country

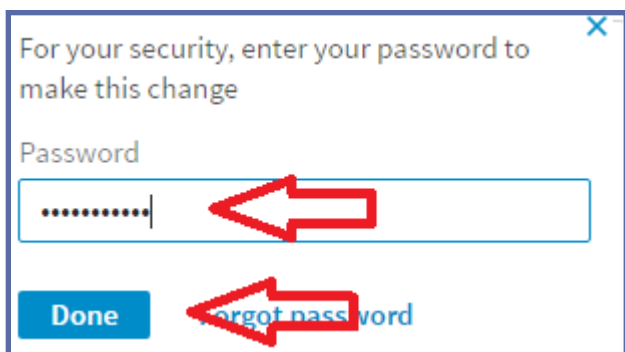
United States

New phone number

8058058056

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

[Cancel](#) [Send code](#)



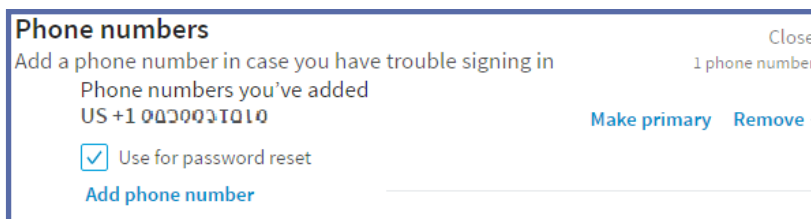
For your security, enter your password to make this change

Password

.....

[Done](#) [Forgot password](#)

9. Check the mobile telephone for a text message from LinkedIn with the verification code. Enter that code and click **Done**.



Phone numbers

Add a phone number in case you have trouble signing in

Phone numbers you've added

US +1 0000001010

☒ Use for password reset

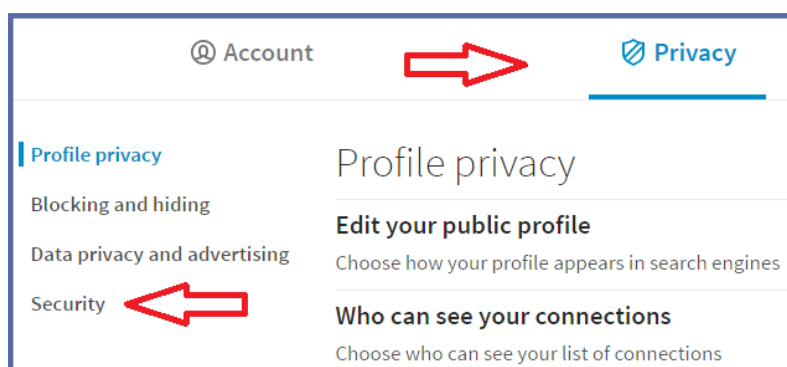
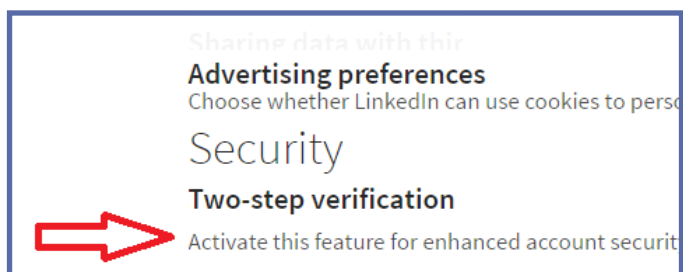
[Add phone number](#)

[Make primary](#) [Remove](#)

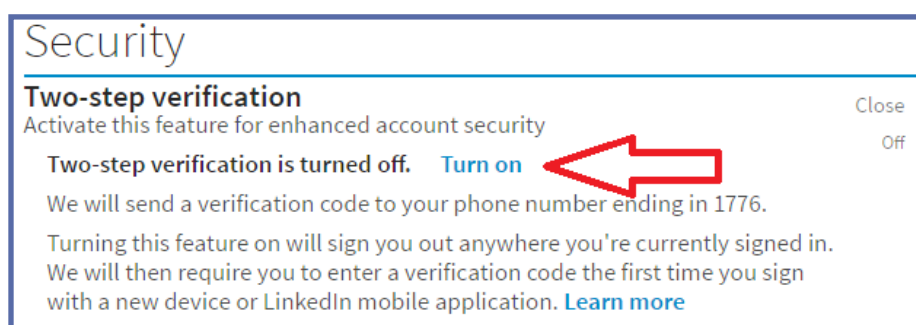
10. If all went well, you'll see a message showing the telephone number you just added to your account.

You're not quite done implementing two-step verification!

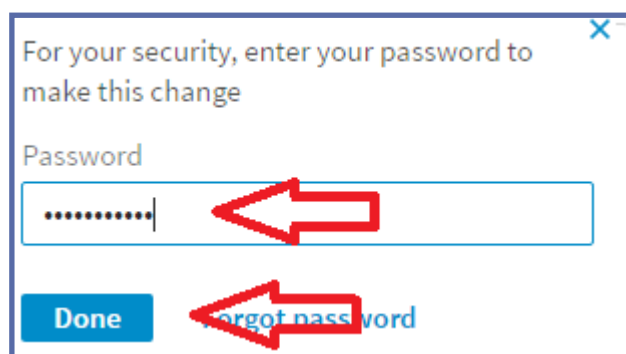
11. Return to the **Privacy** tab and click **Security**.



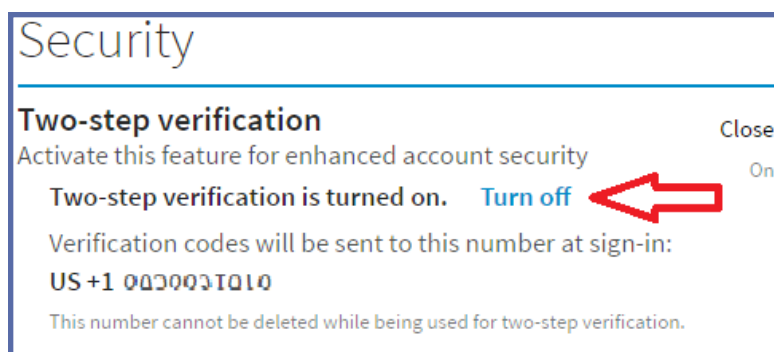
12. Click **Two-step verification**.



13. Click **Turn on**.



14. Enter your password (not the verification code) and click **Done**.



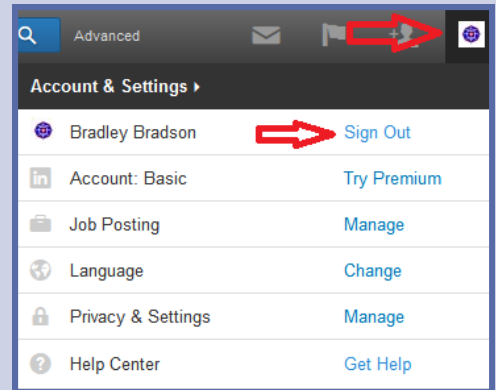
15. The next box will verify that **two-step verification is turned on**.

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.

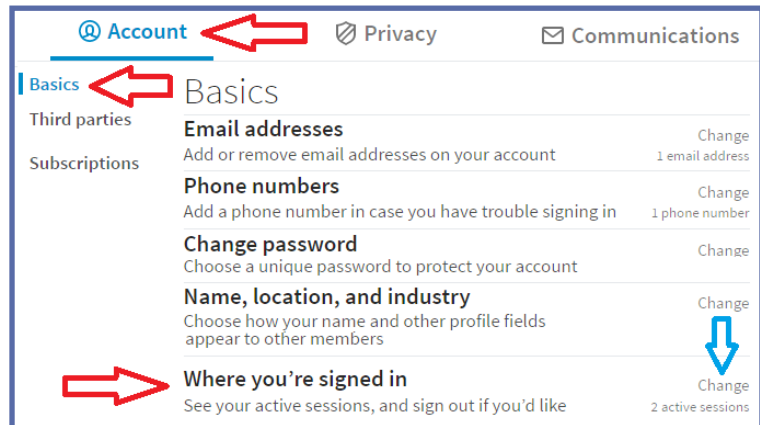
Sign Out When You Finish!
It is Always a Good Security Practice



*Hover your mouse over your profile image and click **Sign Out** when the drop down menu appears*

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

1. Click the **Account** tab.
2. Click **Basics**.
3. Click **Where you're signed in**. Depending upon your screen size, you might have to scroll down a few lines.



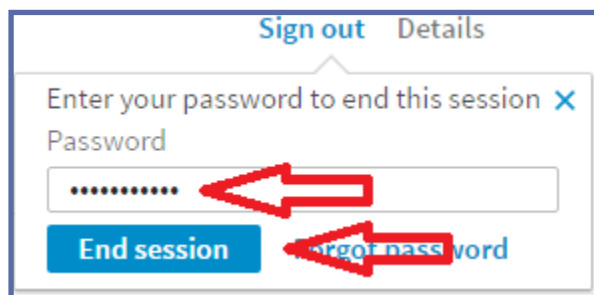
You're currently signed in to 2 sessions.

Here's a list of all the places you're signed into LinkedIn right now. You can see details about each session, sign out of individual sessions, or sign out of everywhere at once. You can also sign out of apps you've authorized with LinkedIn from the **Third party apps** setting.

Current session	Details
	Stafford, Virginia, United States (Approximate location) Chrome on Windows IP Address: 74.93.216.49 IP Address Owner: Comcast Business Communications
Other active sessions (1)	Sign out of all these sessions
Last accessed	Details
13 seconds ago	Stafford, Virginia, United States (Approximate location) Firefox on Windows

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** or **End sessions**.



You're currently signed in to 2 sessions.
Here's a list of all the places you're signed into LinkedIn right now. You can see details about each session, sign out of individual sessions, or sign out of everywhere at once. You can also sign out of apps you've authorized with LinkedIn from the [Third party apps](#) setting.

Current session	Details
	Stafford, Virginia, United States (Approximate location) Chrome on Windows IP Address: 74.93.216.49 IP Address Owner: Comcast Business Communications

6. Verify that the session you intended to end has been ended and there are no new sessions. New sessions could indicate an ongoing compromise.

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 flows. 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 addresses 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 **Accepting Connection Requests** for more details.

Maintaining Your Email Addresses

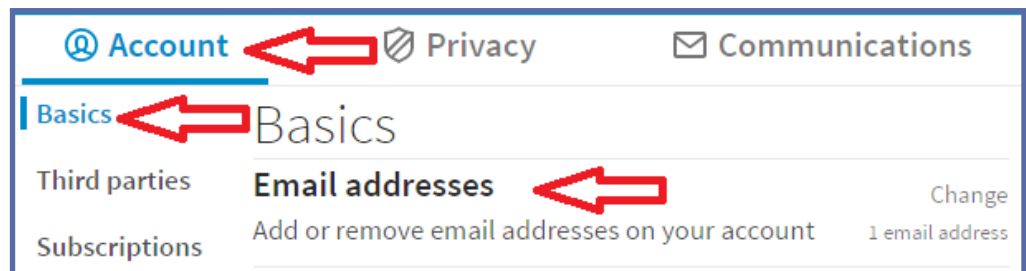
LinkedIn requires that at least one email address be associated with each account and LinkedIn prevents any email address being associated with more than one LinkedIn account. LinkedIn allows you to have multiple email addresses associated with your account, but you will be required to designate one 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 email 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 **Privacy and Settings** menu,

1. Click **Account**.
2. Click **Basics**.
3. Click **Email addresses**.

A screenshot of the 'Email addresses' modal window. It shows a list of 'Email addresses you've added:' with 'brad55@gmail.com' listed as 'Primary'. Below this is an 'Email address' input field containing 'brad54@gmail.com'. At the bottom are 'Cancel' and 'Send verification' buttons. Red arrows point to the input field and the 'Send verification' button.

4. Enter the new address and click **Send verification**.
5. 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's 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 anyone with any of your passwords is contrary to just about every recommended computer security 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.

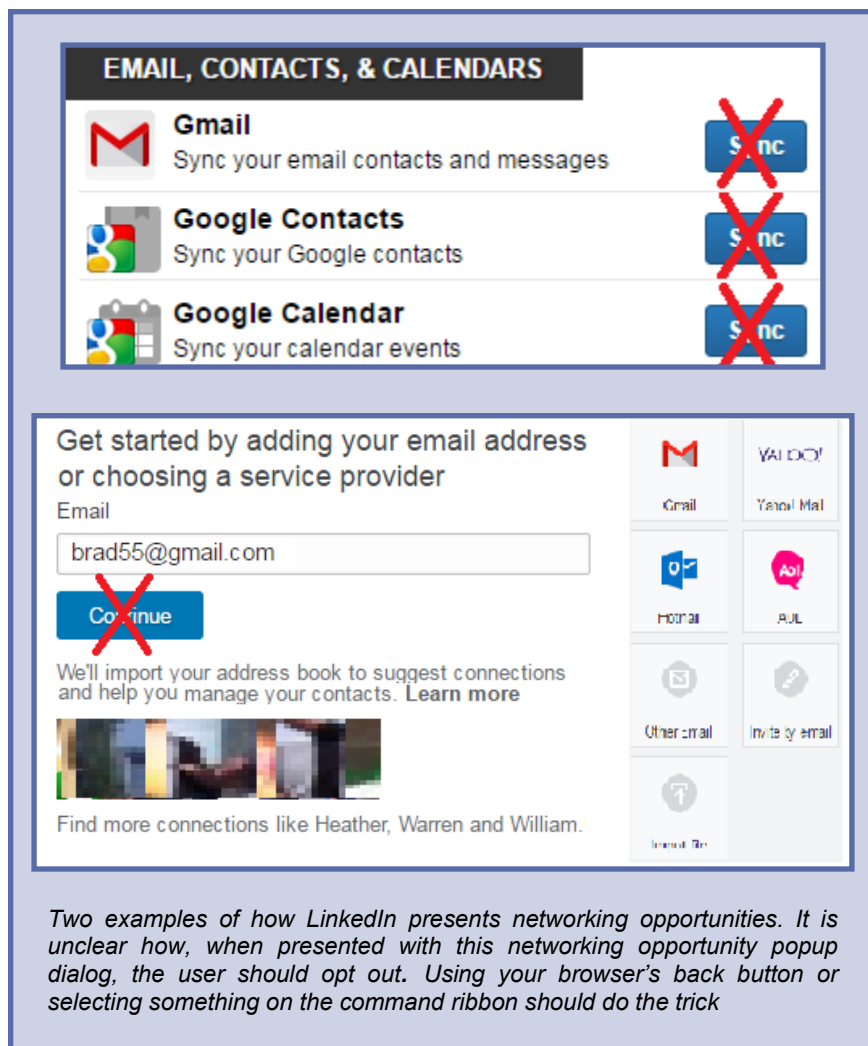
As you use LinkedIn, you will be presented with many opportunities to expand your network. Some opportunities will appear with names and brief biographies of people LinkedIn believes you are associated with. The notices allow easy one-click ways to make connections. Most will be people you know – on 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 **Managing Connections**.)

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 **Managing Connections** 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.

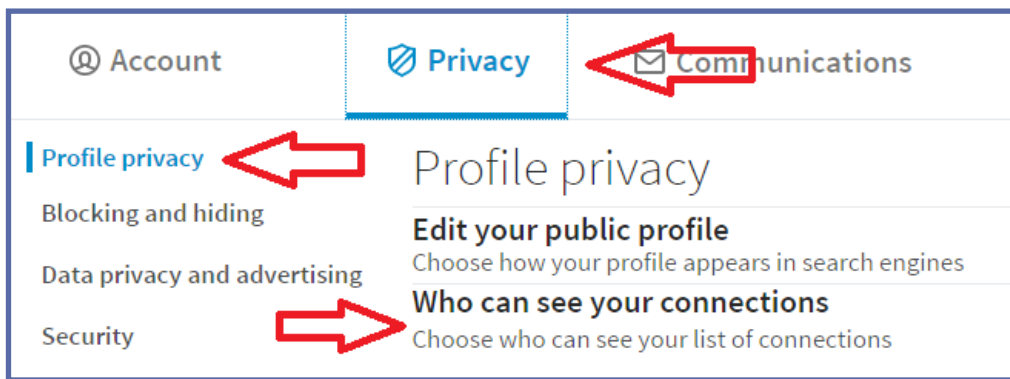


Two examples of how LinkedIn presents networking opportunities. It is unclear how, when presented with this networking opportunity popup dialog, the user should opt out. Using your browser's back button or selecting something on the command ribbon should do the trick

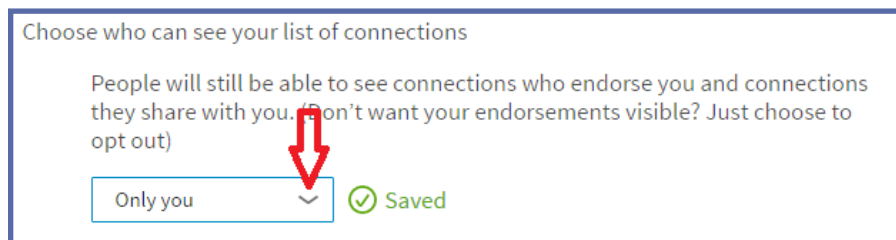
Restricting access to your list of connections is a good practice! Be mindful, however, that even at the most restrictive setting your 1st degree connections will always be able to see mutual connections.

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

1. Click the **Privacy** tab.
2. Click **Profile privacy**.
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**. If a small green checkmark labelled **Saved** appears then the change has been recorded.



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.

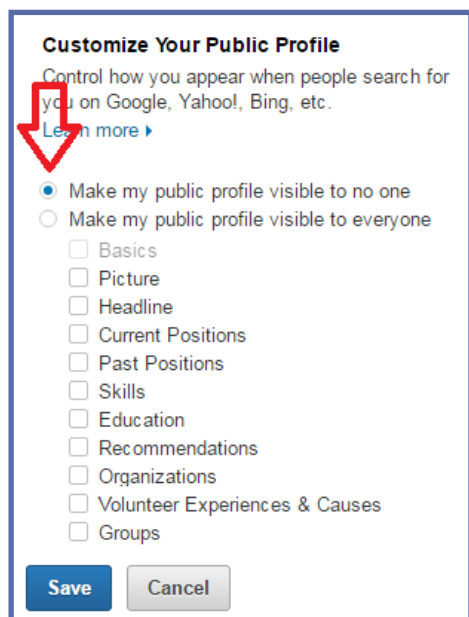
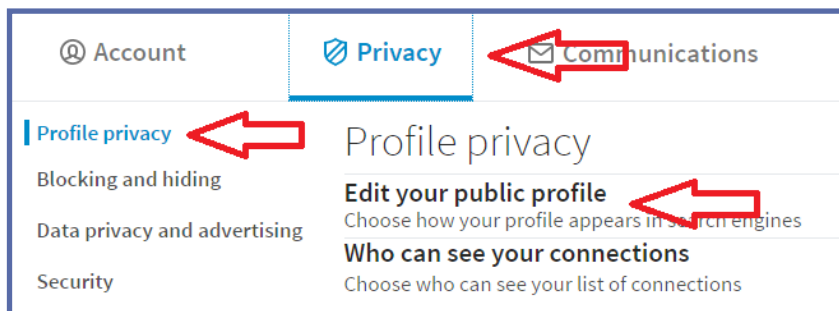
The most restrictive setting is **Make my public profile visible to no one**. With this setting, your profile will still be visible to logged in LinkedIn members: Your profile will not be available to nonmembers, members not logged in and search engines such as Google, Yahoo, Bing, etc.

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.

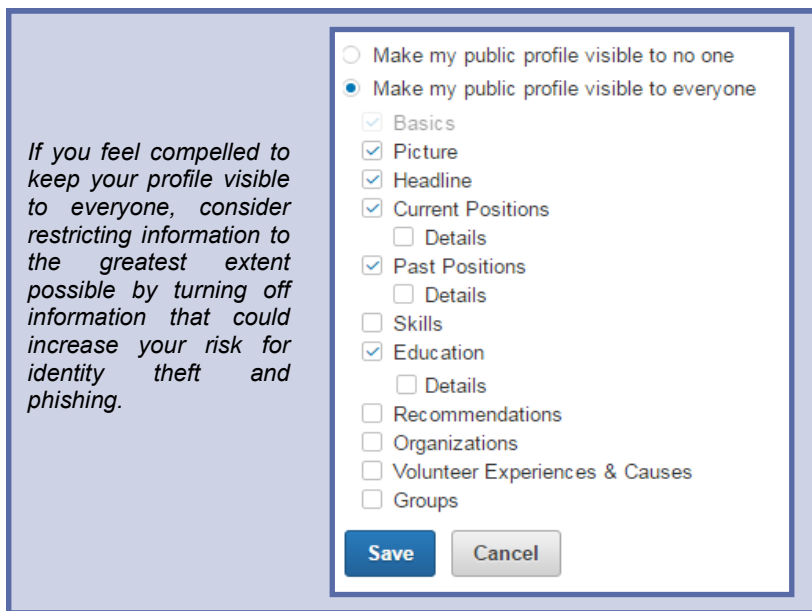
Generally speaking, a recruiter or company seeking candidates would not browse anonymously or without having logged in to LinkedIn. A recruiter would not rely on internet search engines to identify suitable candidates. Therefore, **make my public profile visible to no one** is probably a good choice.

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

1. Click the **Privacy** tab.
2. Click **Profile privacy**.
3. Click **Edit your public profile**.



4. In **Customize Your Public Profile**, select the setting you feel most comfortable with.



** 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.

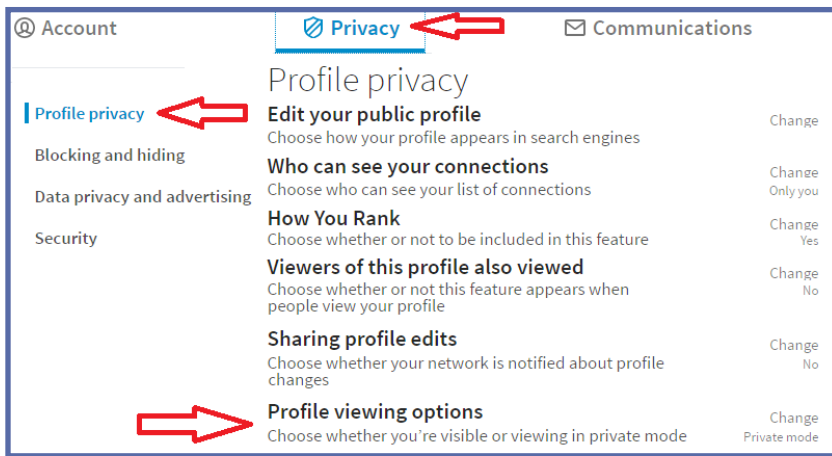
If you choose **Private profile characteristics**, when you browse a connection other than one of your 1st level connections, the only information they will be able to see is your job title, company name (if you listed it) and the industry of your employment. If you have a profile image, that will be replaced by a generic outline of a person. Your name will not appear.

If you choose **Anonymous LinkedIn Member** and browse someone else's profile, that profile owner won't 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.

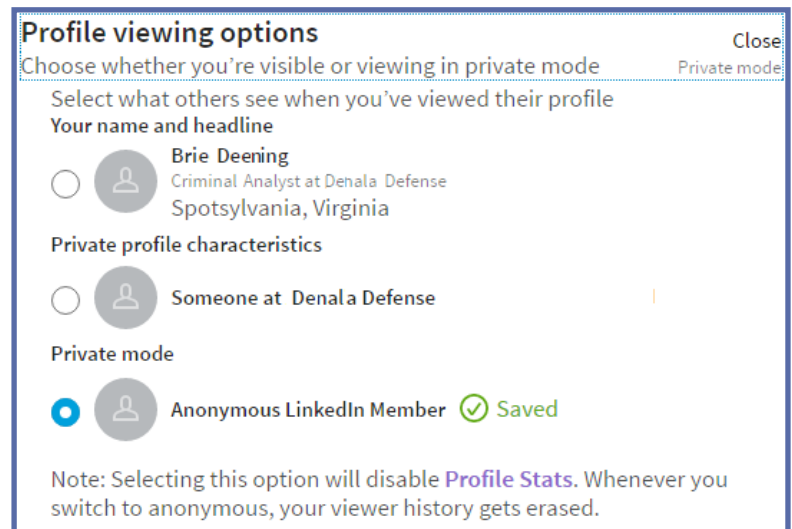
When deciding between **Private profile characteristics** and **Private mode**, consider why you are using LinkedIn and how publicly available you want your information and activities to be.

To change how others see your profile when you browse their profiles, from the **Privacy and Settings** menu,

1. Click the **Privacy** tab.
2. Click **Profile privacy**.
3. Click **Profile viewing options**.



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



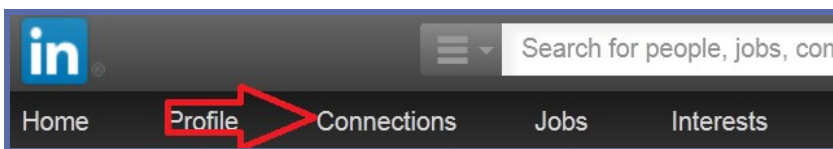
Managing Connections

Removing a Connection, and Blocking or Reporting a LinkedIn Member

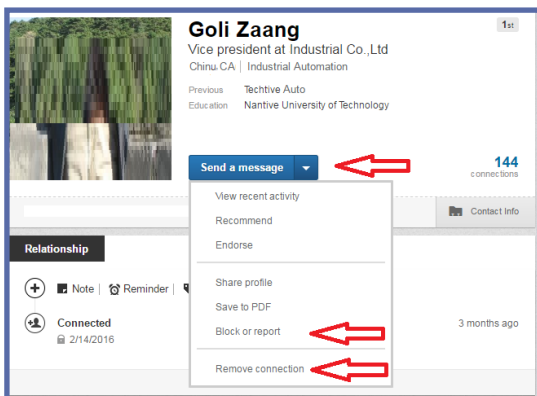
You can remove an existing connection, selectively block any LinkedIn member from viewing your profile or you can report any LinkedIn member for a number of different inappropriate behaviors. If you remove, block or report a user, LinkedIn will not notify that member. If you are connected and block or 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,



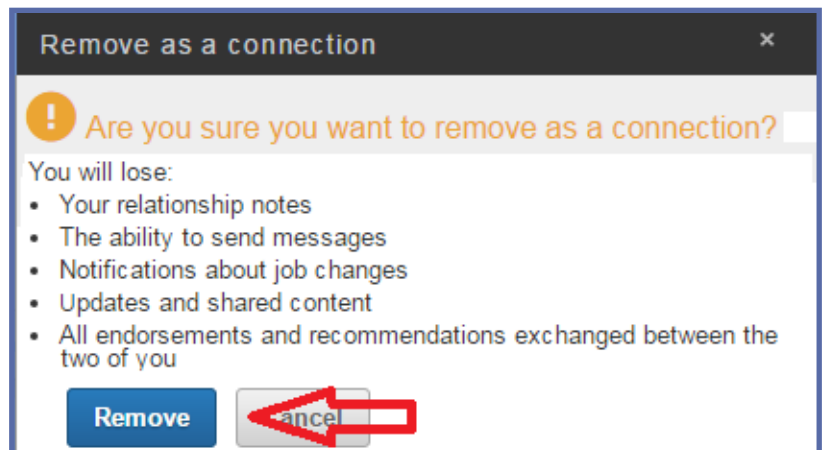
1. Click **Connections** in the command ribbon across the top of your profile.
2. Scroll down and click on the profile name of the person you want to block.



3. Click on the down arrow to the right of **Send a message**.
4. Click **Remove connection** or **Block or report** depending upon your purpose.

If you want to remove the connection then,

1. Click **Remove**.



If you want to **Block** the connection,

1. Click the box opposite **Block**.
2. Click **Continue**.

Block or report this person

Festim Tocilla 2nd
Digital Forensics - Information Security
Philadelphia, Pennsylvania |
Computer & Network Security

☒ **Block Flotsim:**

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore

You can read more about blocking before you agree on the next page.

☐ **Report Flotsim so that:**

This person will be submitted for review. We'll look for inappropriate behavior or violations of our Terms of Use. Choose this option if you think this member's behavior is bad for the LinkedIn community.

Continue **Cancel** [Manage Privacy Settings](#)

3. Read LinkedIn's explanation of the changes you are about to make. If you agree, click **Agree**.

Block or report this person

Festim Tocilla 2nd
Digital Forensics - Information Security
Philadelphia, Pennsylvania |
Computer & Network Security

Are you sure you want to **block** Festim Tocilla?
Here's what will happen:

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore
- We'll remove any endorsements and recommendations from this person
- You'll both stop seeing suggestions to interact

Don't worry - Festim won't be notified. [Learn more about blocking](#)

Blocking someone doesn't change how you appear in public search engines, so **always be aware of the information you share publicly**. You may want to [review your public profile settings](#)

Agree **Go back** [Manage Privacy Settings](#)

If you want to **Report** the connection,

1. Click the box opposite **Report**.
2. Click **Continue**.

Block or report this person

Festim Tocilla 2nd
Digital Forensics - Information Security
Philadelphia, Pennsylvania |
Computer & Network Security

☐ **Block Flotsim:**

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore

You can read more about blocking before you agree on the next page.

☒ **Report Flotsim so that:**

This person will be submitted for review. We'll look for inappropriate behavior or violations of our Terms of Use. Choose this option if you think this member's behavior is bad for the LinkedIn community.

Continue **Cancel** [Manage Privacy Settings](#)

3. In the drop-down menu, select your reason for reporting this connection.

Festim Tocilla 2nd
Digital Forensics - Information Security
Philadelphia, Pennsylvania |
Computer & Network Security

☐ **Block Festim Tocilla so that:**

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore

You can read more about blocking before you agree on the next page.

☒ **Report Festim Tocilla so that:**

This person will be submitted for review. We'll look for inappropriate behavior or violations of our Terms of Use. Choose this option if you think this member's behavior is bad for the LinkedIn community.

Flag profile as: *

an advertisement

Details

I received an unsolicited email from this person.

Continue **Cancel** [Manage Privacy Settings](#)

Festim Tocilla 2nd
Digital Forensics - Information Security
Philadelphia, Pennsylvania |
Computer & Network Security

☐ **Block Festim Tocilla so that:**

- You won't be able to access each other's profiles on LinkedIn
- You won't be able to message each other on LinkedIn
- If you're connected, you won't be connected anymore

You can read more about blocking before you agree on the next page.

☒ **Report Festim Tocilla so that:**

This person will be submitted for review. We'll look for inappropriate behavior or violations of our Terms of Use. Choose this option if you think this member's behavior is bad for the LinkedIn community.

Flag profile as: *

Choose...

Choose...

an advertisement

copyrighted material

inappropriate picture

inappropriate content

misrepresentation

out of date

other

inappropriate background photo

Continue **Cancel** [Manage Privacy Settings](#)

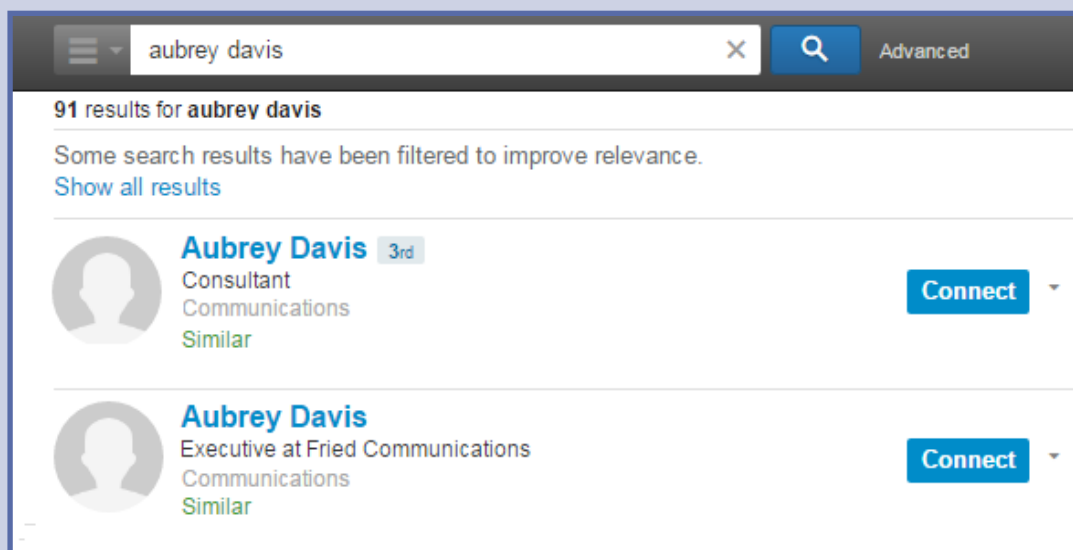
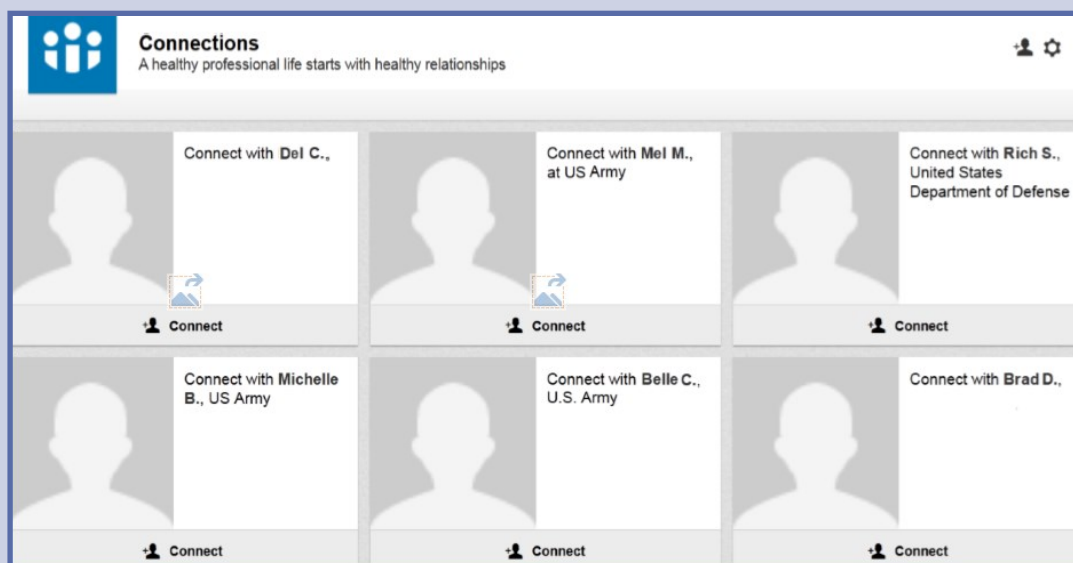
4. Unless your reason for reporting this connection is blatantly obvious, include details about why you are reporting this connection.
5. Click **Continue**.

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.

As mentioned earlier, sharing your address book is generally not a good idea. Unless you feel you fully understand the potential for unpleasant outcomes, do not share any of your address books.

LinkedIn presents opportunities like these to connect with your associates.

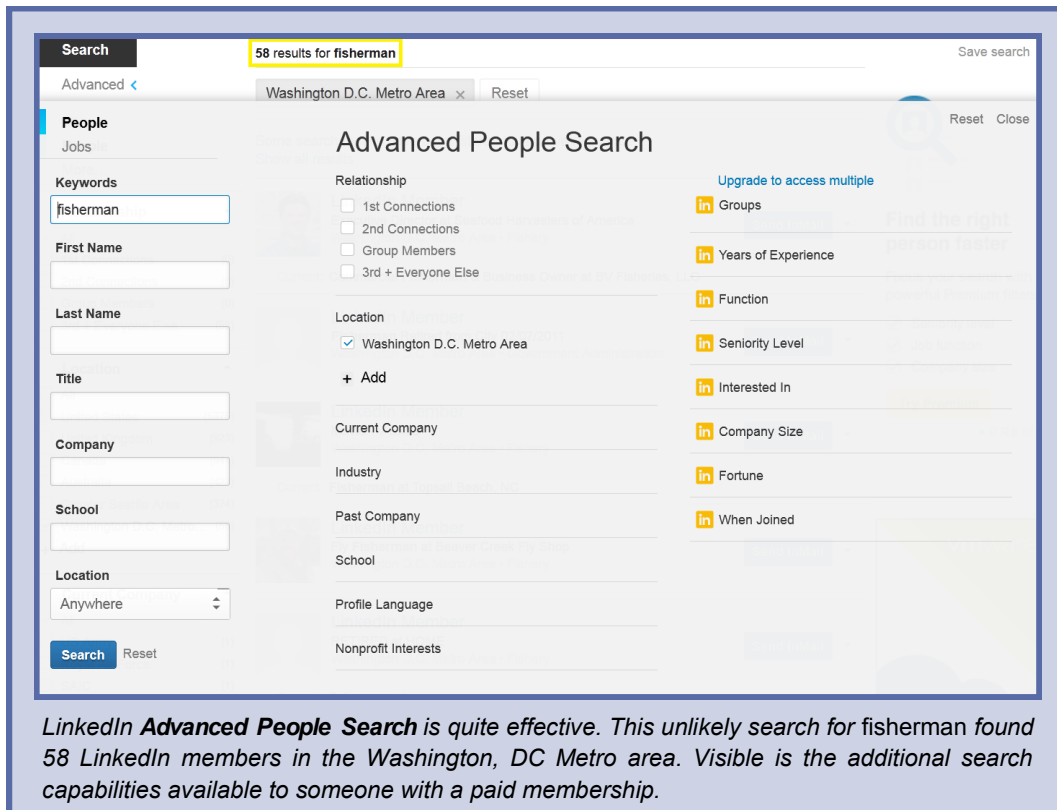
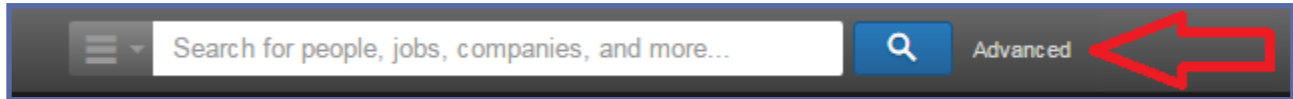


LinkedIn name searches are simple and straightforward and filters present the most relevant results. Exact name searching is not required.

These LinkedIn configuration recommendations are based upon best information available at the time of publication. They are not a guarantee of social networking safety. LinkedIn may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

For a more specific search, or if you want to search for someone with a special or unique background, the **Advanced** search feature can be very effective. Likewise, if a criminal is looking for someone with your unique background, perhaps to exploit or to steal an identity, **Advanced** search is equally effective.

You can access **Advanced** search by clicking **Advanced** to the right of the **Search for people, jobs, companies, and more...**



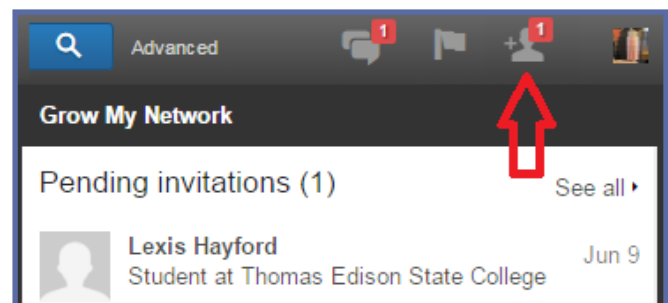
*LinkedIn **Advanced People Search** is quite effective. This unlikely search for fisherman found 58 LinkedIn members in the Washington, DC Metro area. Visible is the additional search capabilities available to someone with a paid membership.*


Accepting Connection Requests

When someone attempts to connect with you, a small number (indicating the number of pending connection requests) appears above the person icon to the left of your LinkedIn profile image.

To accept or reject the connect request,

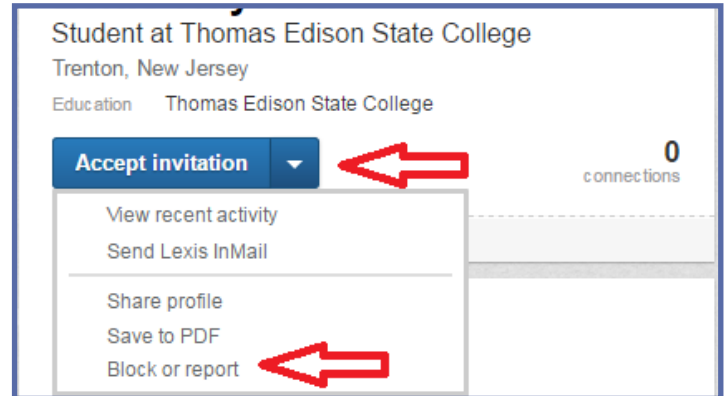
1. Hover your mouse over the person icon. A list of pending connection requests will appear.



2. Hover your mouse over the name of the person whose connection request you want to accept or reject and two symbols appear. 
3. Click the **X** to reject the connection request or click the check mark to accept the connection request.

If you want to block or report the person requesting the connection, there is a means to easily do that.

1. Hover your mouse over the person icon next to your LinkedIn profile image.
2. Click the name of the person whose connection request you want to block or report. This will take you to the person's profile page.
3. Click **block or report**.
4. Follow the instructions in **Removing a Connection, and Blocking or Reporting a LinkedIn Member**.



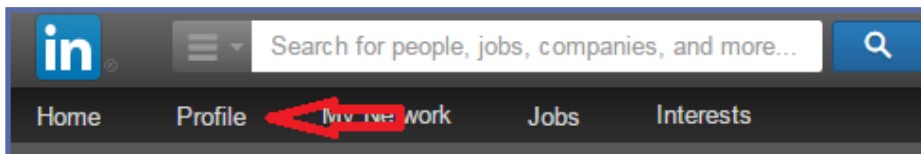
Endorsements and Recommendations

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**).

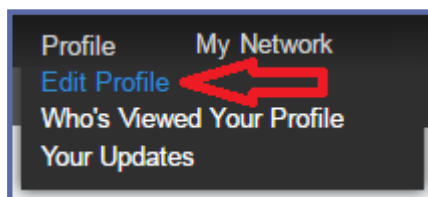
If you have been endorsed for knowledge, skills and abilities that you do not have or if you no longer want an endorsement from a specific individual or for a specific skill, you can delete the endorsement. Your endorser will not be notified of your decision to delete the endorsement. You can also delete 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

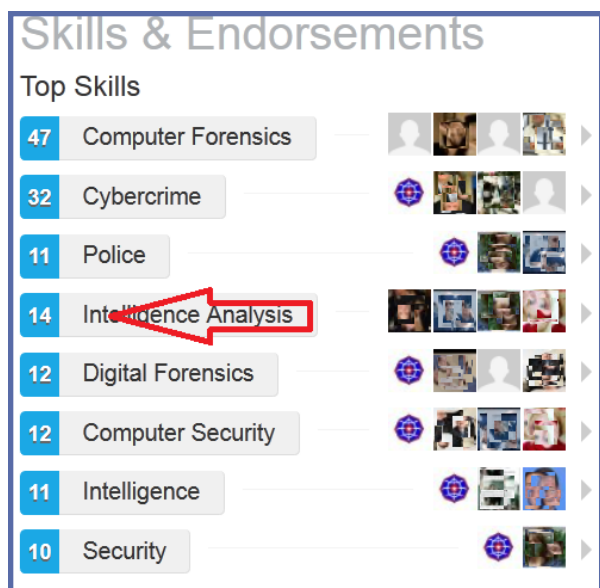
If someone has endorsed you for a skill you do not have or for a skill you do have but would prefer not to broadcast, you can delete that entire skill category.



1. In the command ribbon, click **Profile**.



2. Click **Edit Profile**.



3. Scroll down your profile until you see the **Skills and Endorsements** dialog. Opposite each of the skills are profile images of the LinkedIn members that have endorsed you for that skill.
4. Click any of the listed skills to open a second dialog box.



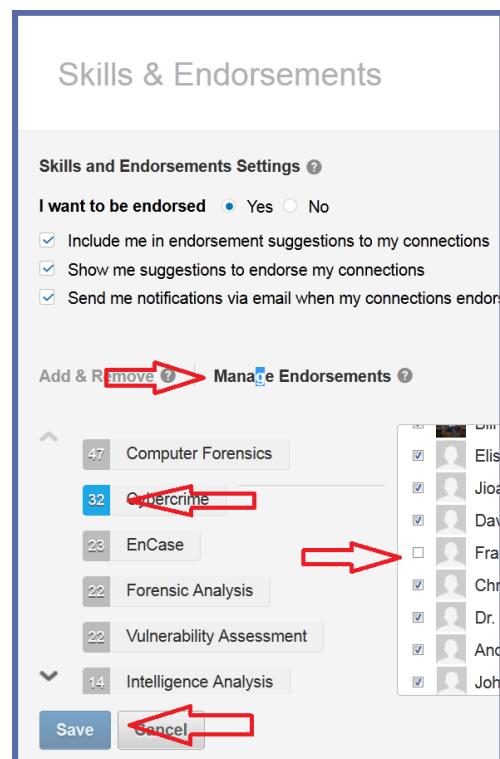
5. Click the **X** by the skill you want to delete.
6. Click **Save**.

Deleting an Individual's Endorsement of You

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

Deleting 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.

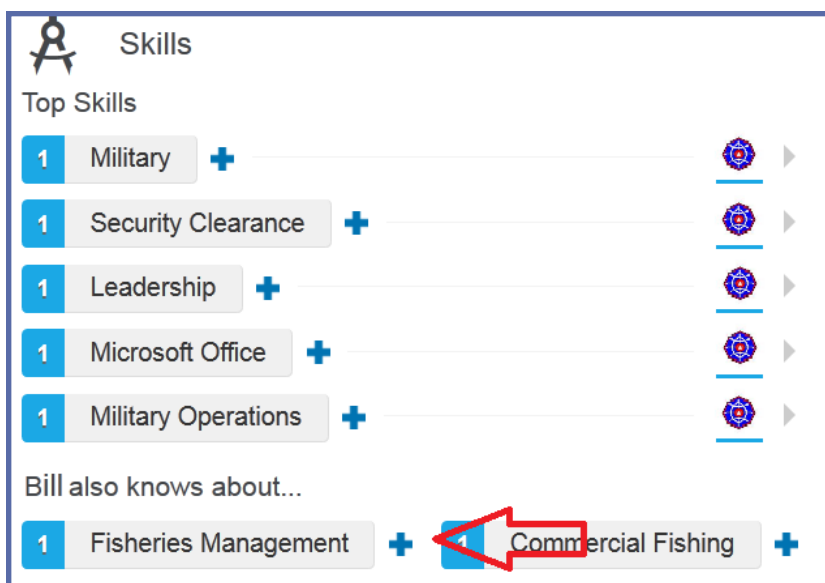
1. From the **Edit Profile** page, scroll down your profile until you see the **Skills and Endorsements** dialog. Opposite each of the skills are profile images of the LinkedIn members that have endorsed you for that skill.
2. Click **Manage Endorsements** at the top of the dialog.
3. Click on the specific category that the individual has endorsed you for.
4. Click the check box opposite the name of the person whose endorsement you want to remove.
5. Click **Save**.



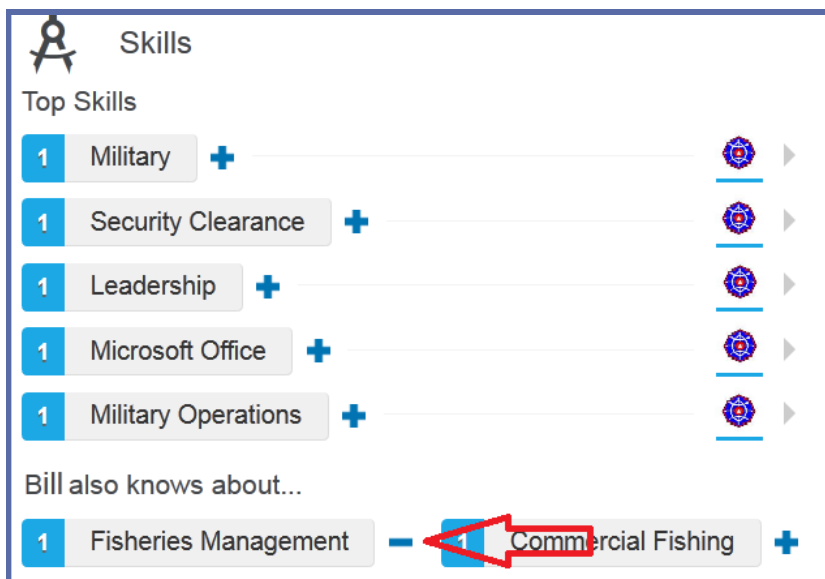
Removing Endorsement You Have Mistakenly Made

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.

1. Navigate to that person's LinkedIn profile page and scroll down to the **Skills** area. Usually, it is in the **Background** section below **Work Experience**.



2. Hover your mouse over the “+” sign to the right of the skill you want to delete. The “+” will change to “-”.



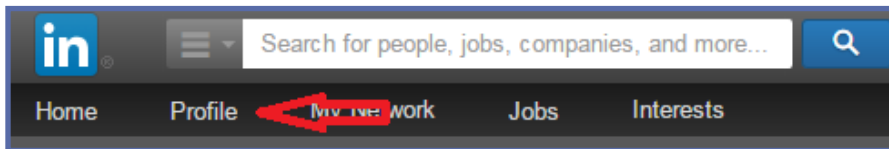
3. Click “-”.
4. The “-” will disappear and be replaced by a grayed out “+”. The skill label may remain but your endorsement for that skill will be gone from their profile.

Hiding Recommendations on Your Profile

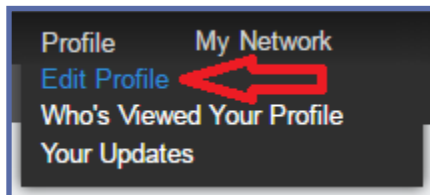
Recommendations appear in your profile near **Skills and Endorsements** and are accessed by editing your profile.

You cannot delete a recommendation once you have accepted it to your profile. You can only hide it from view.

To hide an endorsement:



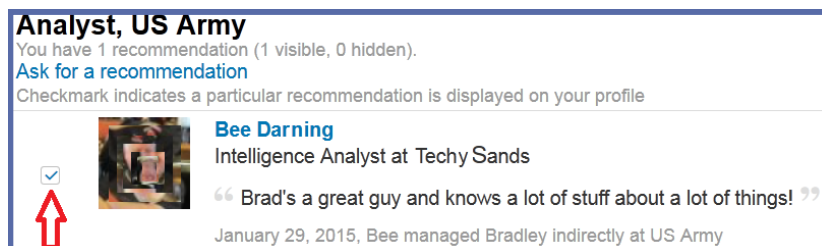
1. In the command ribbon, click **Profile**.



2. Click **Edit Profile**.



3. Scroll down to the **Recommendations** section.
4. Hover your mouse over the upper right corner of the recommendation and click **Manage**.



5. Click on the small box to the left of the profile image. (A small check in the box indicates the recommendation will be hidden from your profile.)
6. There is no specific button to confirm this change. Simply navigate away from this page.

Downloading an Archive of Your LinkedIn Activity

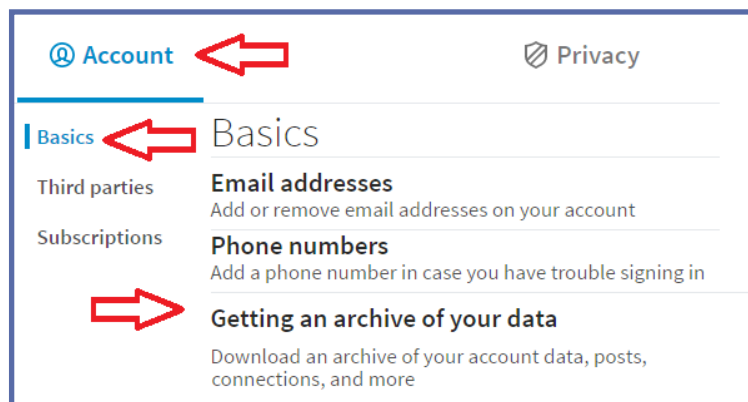
You might find yourself in a situation where you'd like to review all of your LinkedIn activity. Fortunately, there is a means by which you can accomplish this without scrolling through innumerable LinkedIn pages. You can download to your local computer an archive of your information and activity.

Actually, you'll download two archives. The first will be available within a few minutes of submitting the request. It will hold limited information: messages, connections and contacts. That download will be rather small. Within 24 hours a second archive will be available for download. This archive will be much larger and more in-depth.

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 **Privacy and Settings** menu,

1. Click the **Account** tab.
2. Click **Basics**.
3. Click **Getting an archive of your data**. (You might be asked to reenter your password.)



Request your data archive

Download your LinkedIn data

Did you know you can request an archive of your activity and data on LinkedIn anytime?

Within minutes, you'll get the archived information that's fastest to compile including things like your messages, connections and imported contacts. We'll send you an email with a link where you can download it right away.

You'll get an email with a link where you can download the second part of your data archive in about 24 hours. You'll also be able to access your archive by going to your settings, selecting the Account tab, and clicking **Request an archive of your data**. Want more details? Just visit our [Help Center](#).

Here's what's included

Your data archive will contain the information LinkedIn has stored for you including your activity and account history, from who invited you to join, to the time of your latest login. For the full list, visit our [Help Center](#).



Request archive

4. Click **Request archive**.

This message let's you know your LinkedIn activity is being collected and assembled and will be ready for download soon.

Success! Your data is being prepared for download.

What's on its way? In a few minutes you'll get an email with a link where you can download the first installment of the archived information we have for you on LinkedIn including your messages, connections, and imported contacts.

Within 24 hours, we'll send you another email with a link where you can download the second part of your archive. It'll include your activity and account history, from who invited you to join to the last time you logged in. Want to see the full list of what's included? Just visit our [Help Center](#).



Request pending

5. Periodically check the inbox of the email address associated with your LinkedIn account. Look for a message indicating your first data download is available.
6. Return to LinkedIn.
7. Click **Download**.

The first installment of your data is ready!

Here's just the first part of the information we have archived for you, including things like your messages, connections, and imported contacts. You can download it from the link on the right.

Within 24 hours, you'll get an email with a link where you can download the second part of your archive. It'll include your activity and account history from who invited you to join to the last time you logged in. Want to see the full list of what's included? Just visit our Help Center.



Download

Remember. Your LinkedIn archive is actually two files. The first file is available very quickly. It's the file you just downloaded. Data for the second, more extensive file is still being collected.

The second part of the archive of your data is ready!

You can download it from the link on the right anytime over the next three days. For security reasons, you shouldn't share the link, and you should only download it to your own computer. Want more info? Just visit our Help Center.



Download

1. Periodically check your inbox for a message telling you your second archive file is available.
2. Return to LinkedIn.
3. Click **Download**.

Return to [Social Networking Safety Tips](#)

ICE

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

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flier (CCPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this CCPF.