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

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]
E-mail:
usarmy.cciuintel@mail.mil

CCIU Web Page:
www.cid.army.mil/cciu.html

"Do What Has To Be Done"

CPF 0037-14-CID361-9H-LinkedIn* 10 March 2015

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 or sorority brothers or 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 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 for themselves how to balance privacy, security and safety against the value of building a successful business network. Accordingly, these configurations 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 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. Therefore, 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 number of free and completely anonymous email providers.

* This LinkedIn configuration guide is an addendum to CID Crime Prevention Flyer CPF-0037-14-CID361-9H

LinkedIn does offer paid memberships tailored for 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 or ban a connection request is an important decision. Likewise, deciding who to connect with is equally important.

Since LinkedIn attracts professionals, people in positions of responsibility and trust, like you, its members may be a more attractive target for criminals. Therefore, you should consider the following:

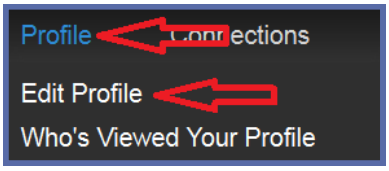
- Do not include in your profile that you have the keys to the kingdom or a security clearance.
- Exercise appropriate skepticism when contacted by someone not known to you regardless of how credible their LinkedIn presence appears. Not everyone on the internet is who they say they are.
- Be cautious when considering accepting a connection request from those you do not know.
- Be cautious when considering accepting a connection request because the requestor's network includes people you know only tangentially.
- Seek and accept connections that add quality to you 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 available from one of two locations along the command ribbon: **Edit Profile** and **Privacy and Settings**. Throughout this document, you will be directed to one of these two areas to access the various settings.

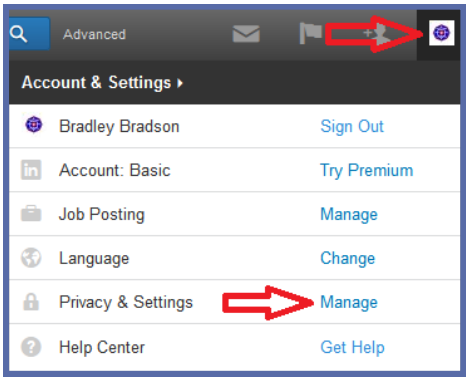
Edit Profile

To access your profile, hover your mouse above **Profile** in the command ribbon and click **Edit Profile** when it appears.



Privacy and Settings

To access **Privacy and Settings**, hover your mouse above the profile picture and when the **Accounts & Settings** menu appears, click **Manage**.



Cyber Crime Prevention Flyer

Controlling Access to Your LinkedIn Account

Passwords

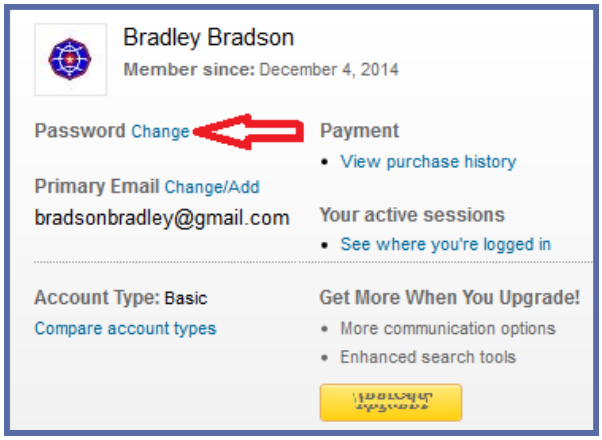
Passwords, secret elements of authentication, are on the front line of defense preventing people and automated tools (e.g., password crackers) from illegally accessing your online accounts. Therefore, your choice of password and the frequency with which you change it are important security considerations.

A password, however, need not be limited to a word. It can be a passphrase. A passphrases 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 a single password.

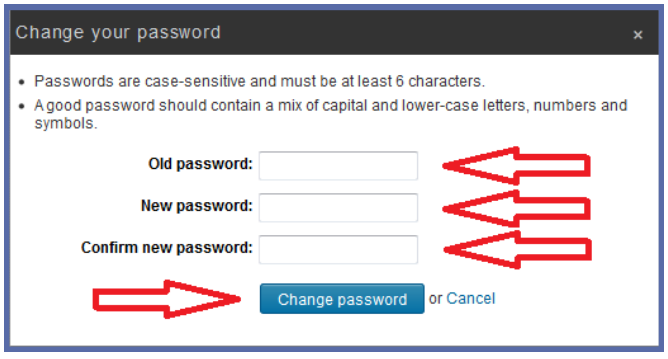
Changing passwords is a straightforward process. A good security practice is to change your password from time to time and is an absolute necessity if you believe your profile has been compromised.

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 keyboard



1. To the right of **Password**, click **Change**.



2. Enter your **Old password**.
3. Enter your **New password**.
4. **Confirm** your **new password**.
5. Click **Change password**.

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.

Cyber Crime Prevention Flyer

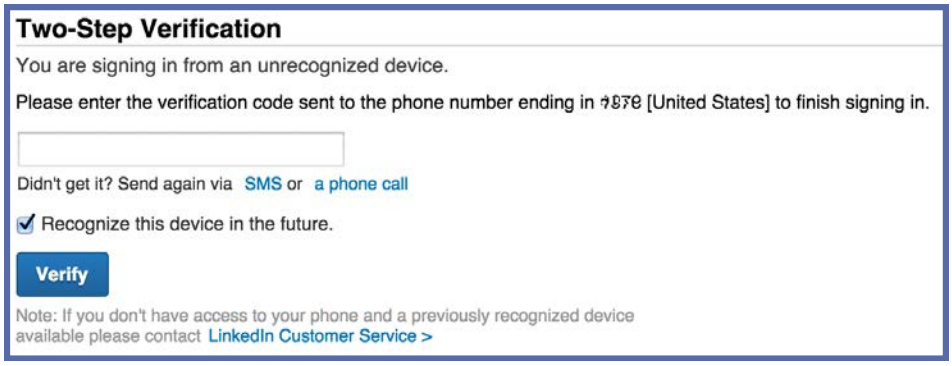
Two Step Verification

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 as a text message, 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, this can create challenges with **Two Step Verification** feature.

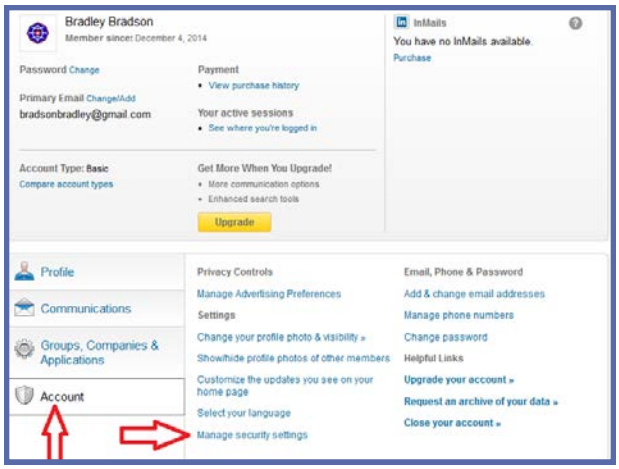
The defensive benefit of **Two Step Verification** is the text message you receive notifying you of access from a not yet authorized browser. If you receive a login notification and are not trying to log in, there is a strong possibility someone is trying to access your LinkedIn account. If you believe this to be the case, you should immediately follow the steps in **See Where You're Logged In**.



IMPORTANT: If you are logging in from a public or shared computer DO NOT check **Recognize this device in the future.**

To activate **Two Step Verification**, from the **Privacy and Settings** menu:

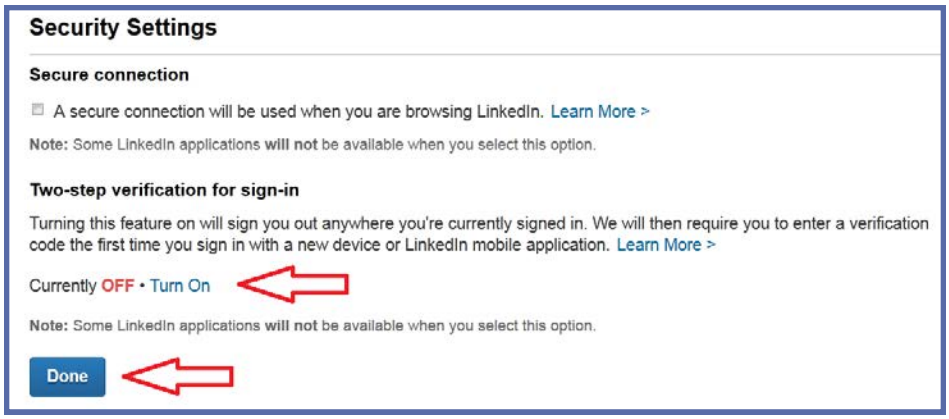
1. Click **Account**.
2. Click **Manage security settings**.



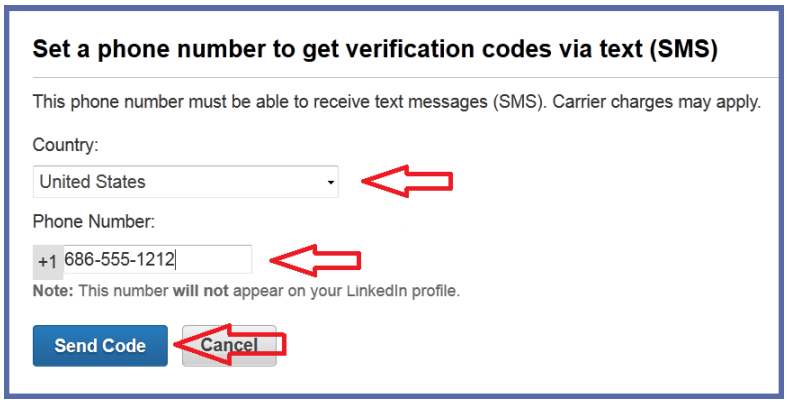
These LinkedIn configuration recommendations are based upon best information available at the time of publication. They are not a guarantee of social networking safety. LinkedIn may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

Cyber Crime Prevention Flyer

3. Under **Two-step verification for sign-in** click **Turn On**.
4. Click **Done**.

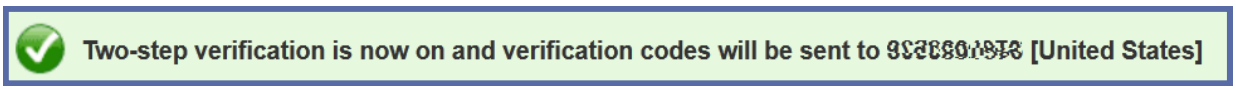


5. Verify the **Country** is set correctly.
6. Enter the mobile telephone number to which you want verification messages sent.
7. Click **Send Code**.



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

9. If all went well, you will notice a green banner near the top of the dialog box announcing the setup was successful.



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.

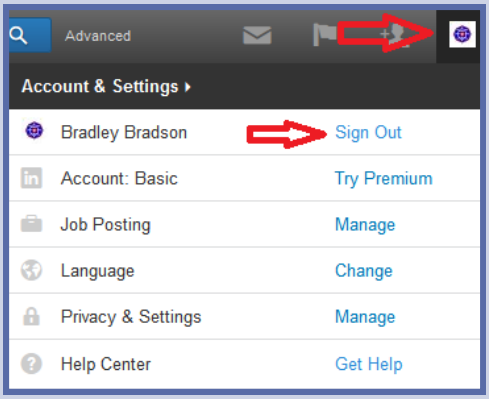
Cyber Crime Prevention Flyer

See Where You're Logged In

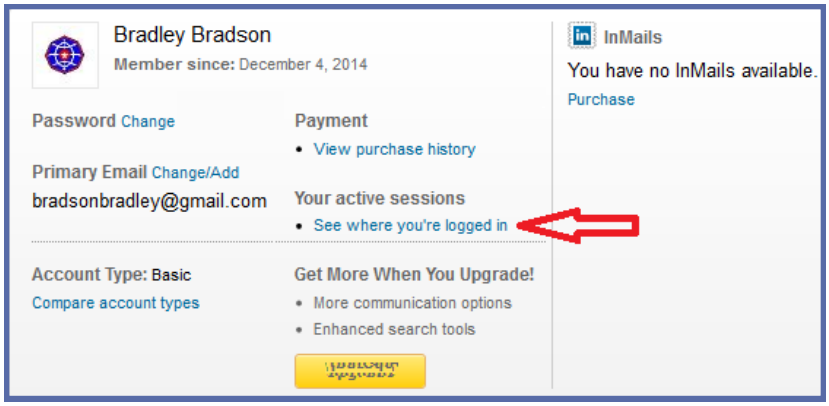
This feature can be used to end any active LinkedIn session. This is more of a security audit tool than a security measure. It will not prevent the compromise of your account but it can tell you if unauthorized access to your account is occurring and may indicate a past compromise. **See Where You're Logged In** will also help you to identify LinkedIn sessions that were not properly closed.

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 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.

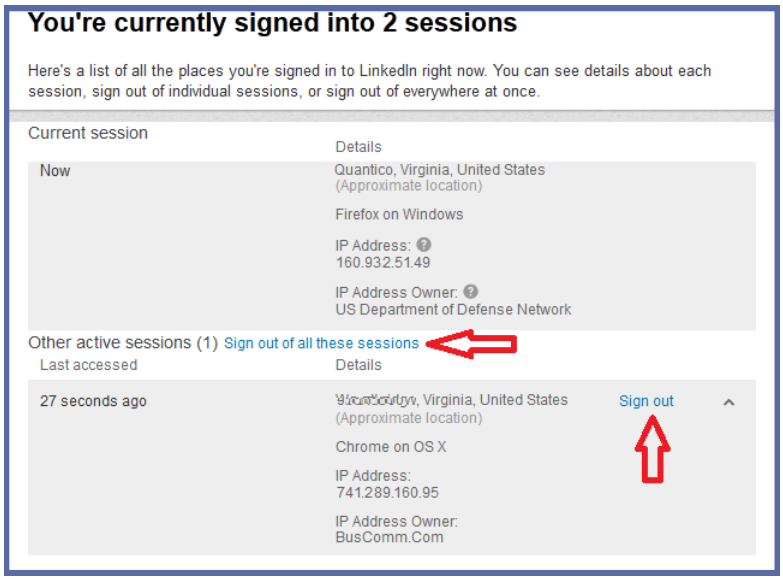
***Sign Out** When You Finish!*
It is Always a Good Security Practice.



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



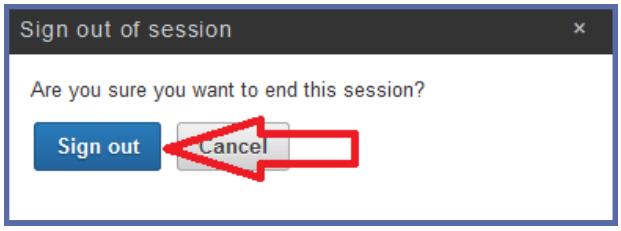
1. From the **Privacy and Settings** menu, click **See where you're logged in**.



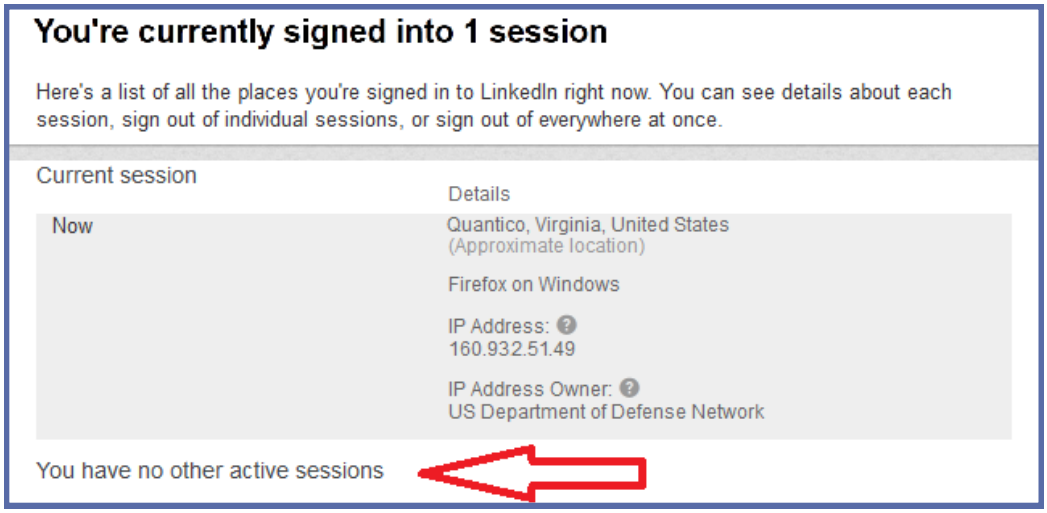
2. Identify session locations that you want to terminate and click **Sign out**. If you find yourself logged in from multiple sessions you can terminate them all by clicking **Sign out of all of these sessions**.

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.

Cyber Crime Prevention Flyer

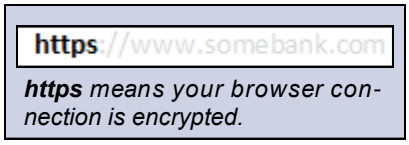


3. Click **Sign out**.



4. Verify there are no new sessions. New sessions could indicate an ongoing compromise.

Secure Connection



Choosing secure browsing is rarely a bad idea. Enabling this feature will activate Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) and your information will be encrypted as it travels from computer to computer. Most legitimate websites enable HTTPS whenever personal or sensitive information (credit cards, passwords and user names, etc.) is being transferred. When your browser has gone secure you will see “https” in your browser address bar.

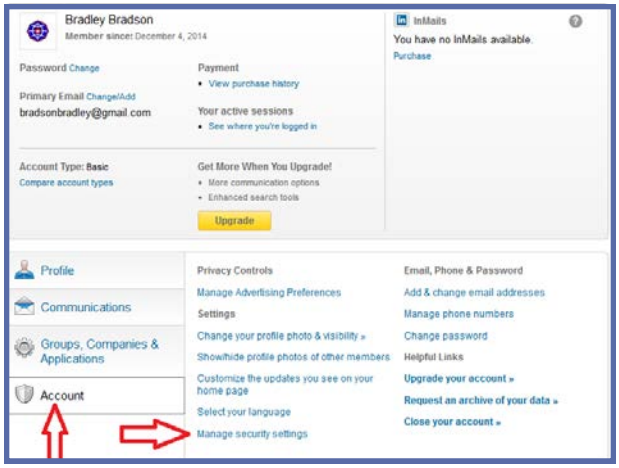
If you regularly access LinkedIn from WiFi hotspots or public computers (e.g., hotel business centers, Internet cafés and the like), you should enable this feature. With this setting enabled, all of your LinkedIn activity will be encrypted while transiting the Internet.

However, if you are a frequent LinkedIn user or a power user there may be a downside. According to LinkedIn:

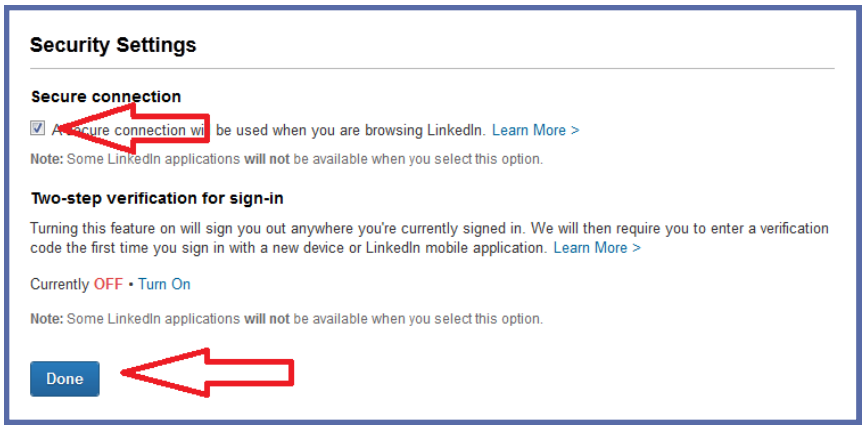
> Supporting HTTPS across the entire site is still a work in progress. There are portions of our site that include content from third parties who may not support https. On these pages, browsers may display a warning or notification. We are working to fix these issues, and meanwhile we want our members to have the option to browse the web securely.

If the frequency of these notices becomes onerous or you are prevented from accessing features you need, then disabling this feature may be the best choice for you.

Cyber Crime Prevention Flyer



1. From the **Privacy and Settings** menu, click **Account**.
2. Click **Manage security settings**.



3. Click the box below **Secure connection**. This feature is enabled when there is a checkmark in the box and disabled when the checkmark is missing.
4. Click **Done**.

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, do not use your official Army email address for your personal LinkedIn account. Army Memorandum 09-026 (25 FEB 10) prohibits the use of government email addresses and government logos to establish personal accounts. 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.

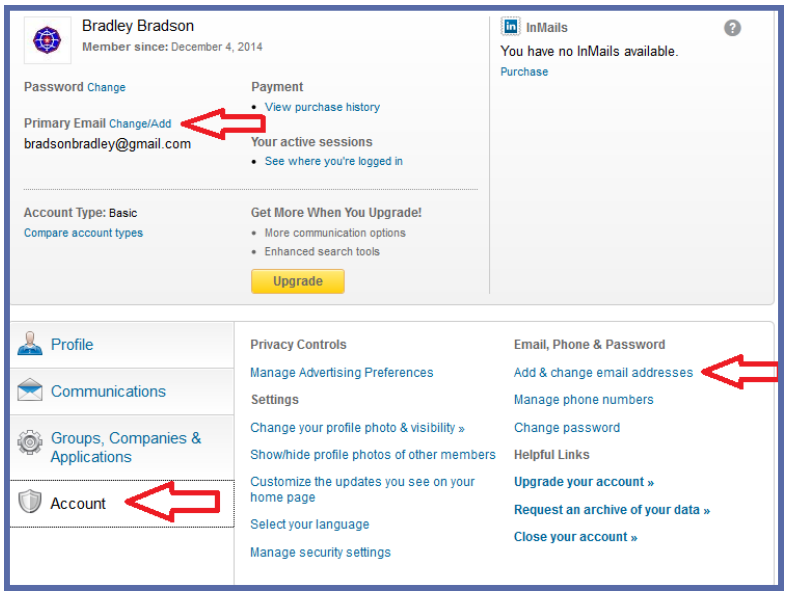
The email address you use will be visible to your 1st degree connections. Therefore, it is important to be selective about who you accept as connections. (For more information, see **Accepting Connection Requests**.)

Cyber Crime Prevention Flyer

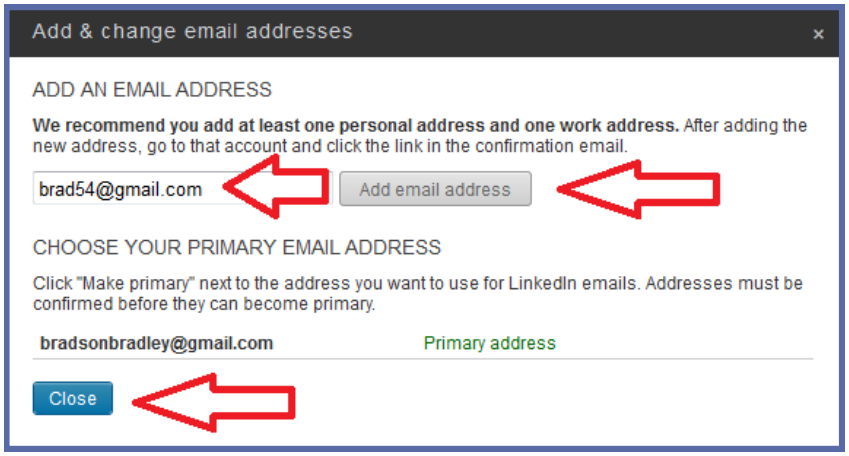
Maintaining Your Email Addresses

LinkedIn requires that an email address be associated with each account and LinkedIn prevents an email address from 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.

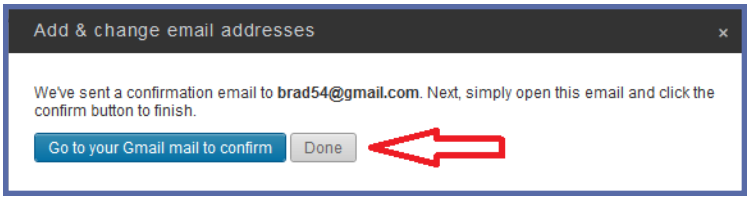
You can delete any associated email address except your primary email address. In order to delete your primary address, you must first add and then designate as primary a new email address. Whenever you add a new email address, LinkedIn sends a verification email to it. The final connection to your profile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



1. From the **Privacy and Settings** menu, opposite **Primary Email**, click **Change/Add** or click **Account** and click **Add & change email addresses**.



2. Enter the new address and click **Add email address**.
3. Click **Close**.



4. Click **Done**.
5. Check the email inbox for a LinkedIn email and follow the instructions there to activate the new email address.

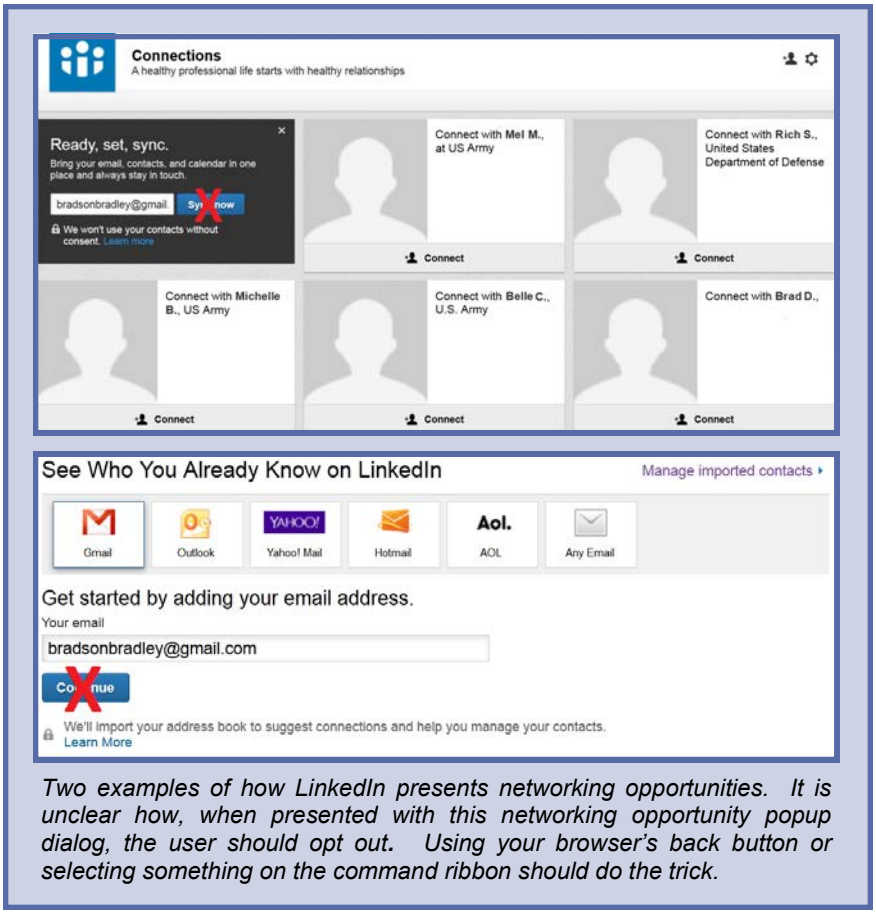
Cyber Crime Prevention Flyer

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 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 anyone with any of your passwords is contrary to just about every recommended computer security practice. 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.



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.

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. (For more information, see **Making Connections**.)

Profile Settings

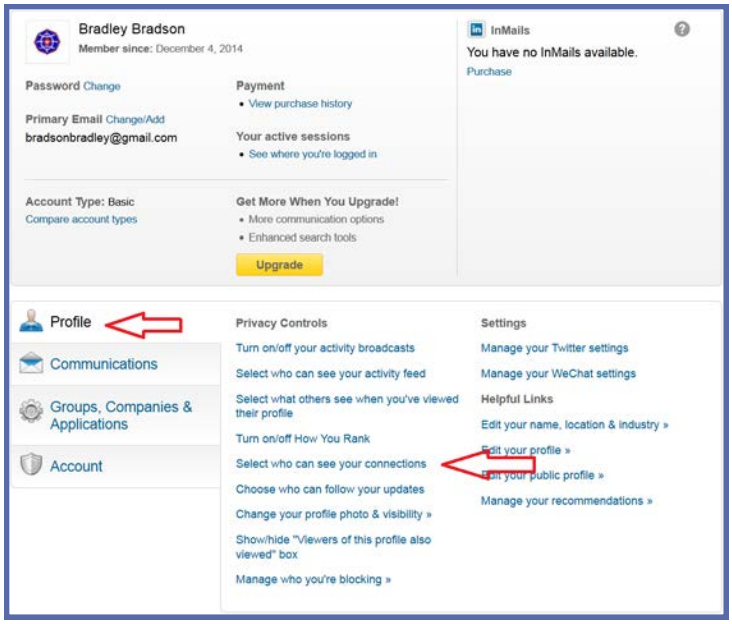
Your **profile** says everything about you. It is your LinkedIn presence. Take care with what you post and remember that first impressions are everything.

Controlling Who Can See Your Connections

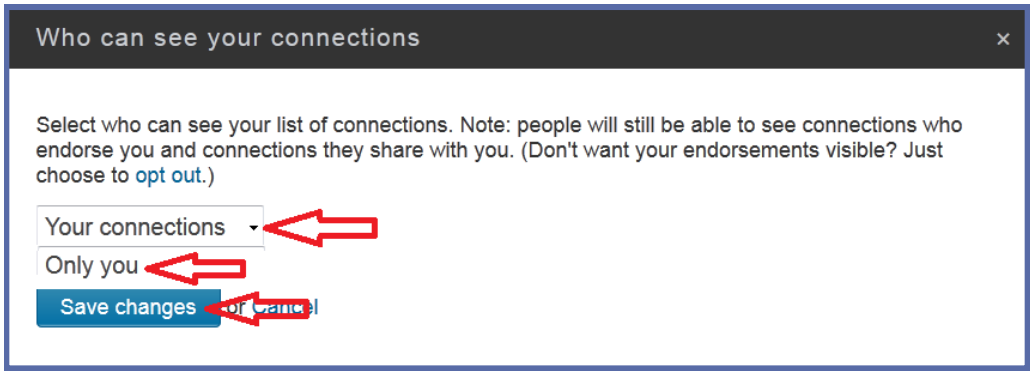
If you have properly managed your connections (you will find more information about managing connections in the Managing Connections section), then your list of connections says a lot about who you are. That list also contains information that can be exploited by someone with a mind to do so. By default, 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.

Cyber Crime Prevention Flyer



1. From the **Profile and Settings** menu, click **Profile** and click **Select who can see your connections**.



2. Click the **Option Arrow**.
3. Click **Only you**.
4. Click **Save changes.**

Limit Public Access to Your Profile

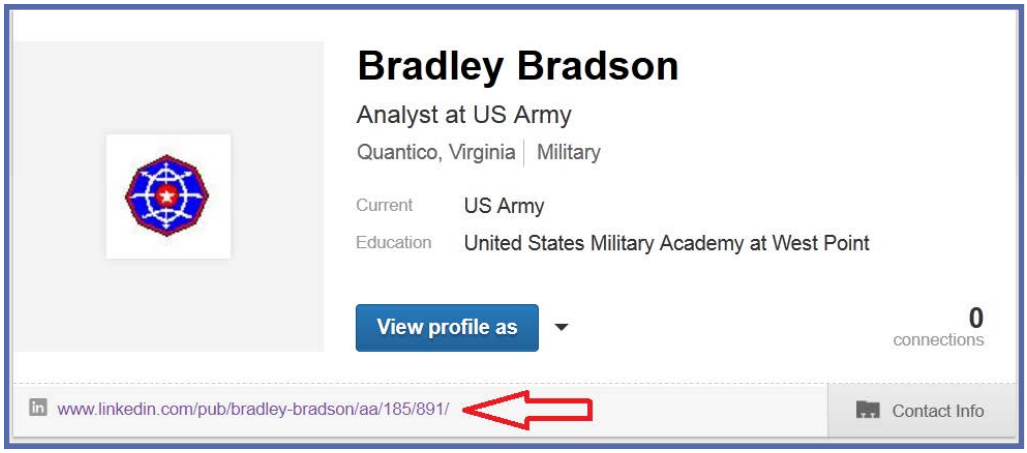
When you restrict access to your LinkedIn profile to only logged in LinkedIn members, you not only reduce your attack surface but you prevent its being indexed by search engines.

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.

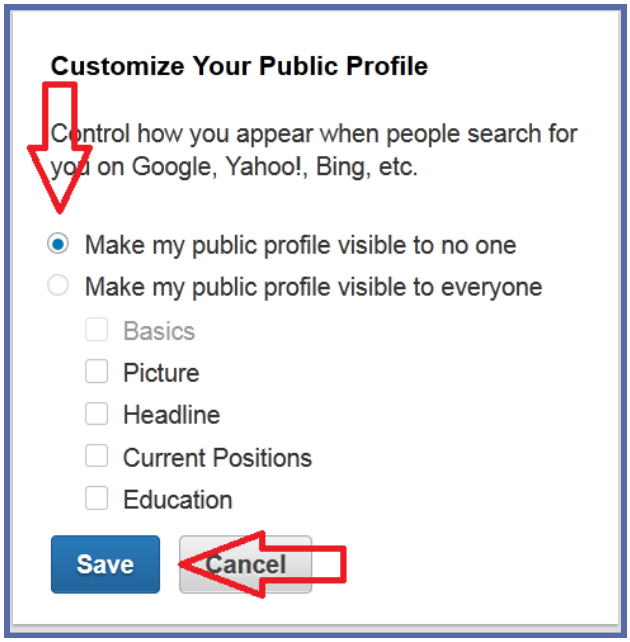
When deciding upon a setting, consider why you are on LinkedIn. Perhaps you want people to be able to locate your profile using an Internet search site. Perhaps you do not. Perhaps you want your profile to be viewable to people who are not LinkedIn members. Perhaps you do not.

Cyber Crime Prevention Flyer

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.

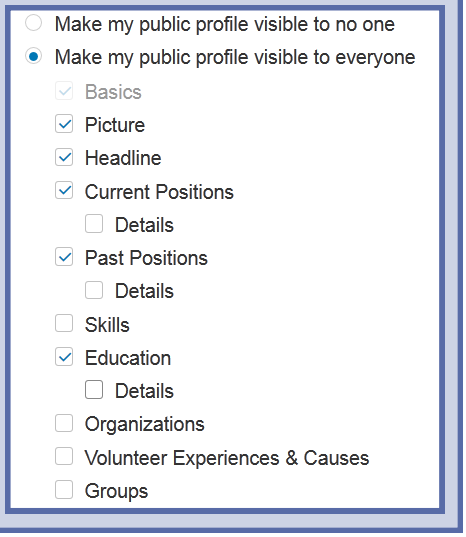


1. From the **Edit Profile** page, click the personal url below your profile image.



2. Click **Make my public profile visible to no one**.*
3. Click **Save**.

If you feel compelled to keep your profile visible to everyone, consider restricting information to the greatest extent possible by turning off information that could increase your risk for identity theft and phishing.



** Information already indexed by search engines will persist for an indefinite period of time.*

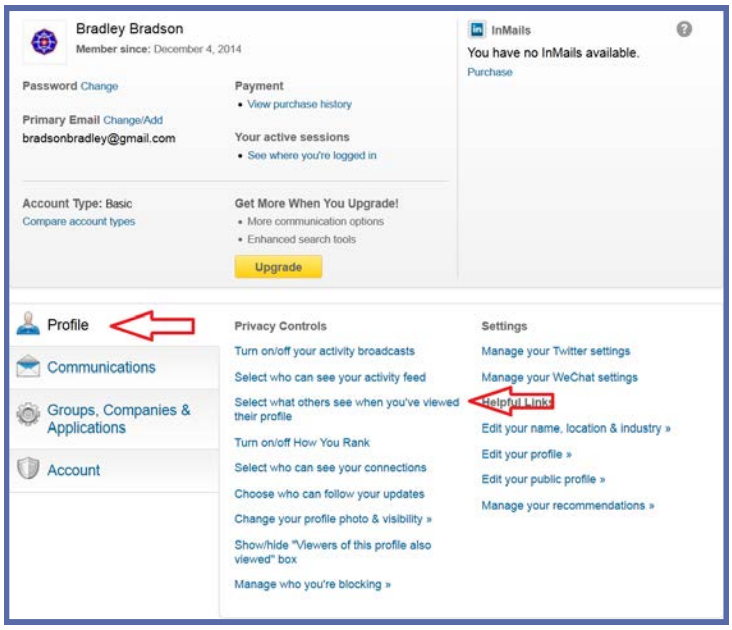
These LinkedIn configuration recommendations are based upon best information available at the time of publication. They are not a guarantee of social networking safety. LinkedIn may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

Cyber Crime Prevention Flyer

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 information. 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.

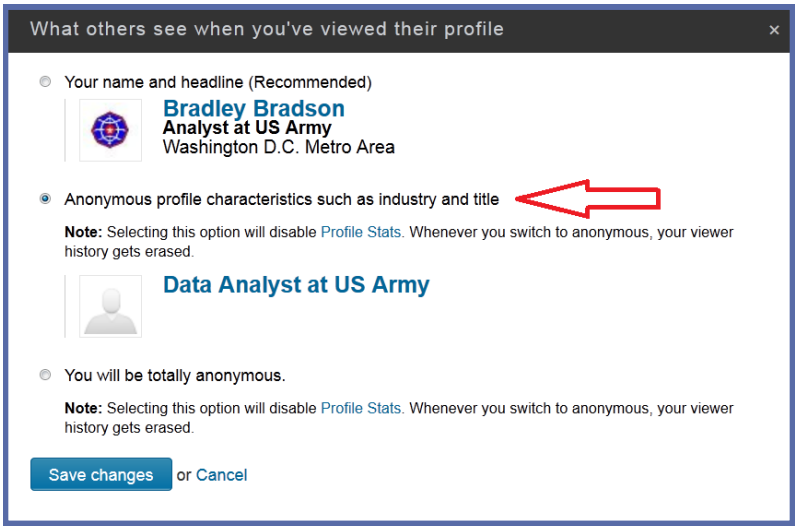
Regardless of this setting, your full name and profile image will be visible whenever you browse the profile of one of your 1st level connections.



If you choose **Anonymous profile characteristics such as industry and title**, when you browse a connection other than one of your 1st level connection's, the only information they will be able to see is your job title and the industry of your employment. If you have a profile image, that will be replaced by a generic outline of a person.

If you choose **You will be totally anonymous** 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 **Anonymous profile characteristics such as industry and title** and **You will be totally anonymous**, consider why you are using LinkedIn and how publicly available you want your information and activities to be.

1. From the **Privacy and Settings Menu**, click **Profile**.
2. Click **Select what others see when you've viewed their profile**.



3. At a minimum, change the setting to **Anonymous profile characteristics such as industry and title**.

   For an even greater level of security, click **You will be totally anonymous**.

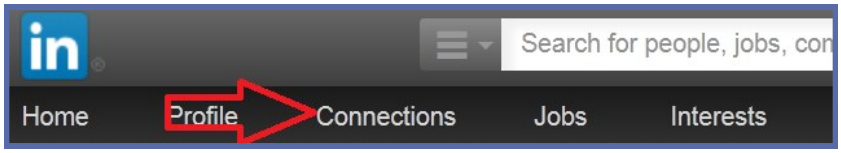
Cyber Crime Prevention Flyer

Managing Connections

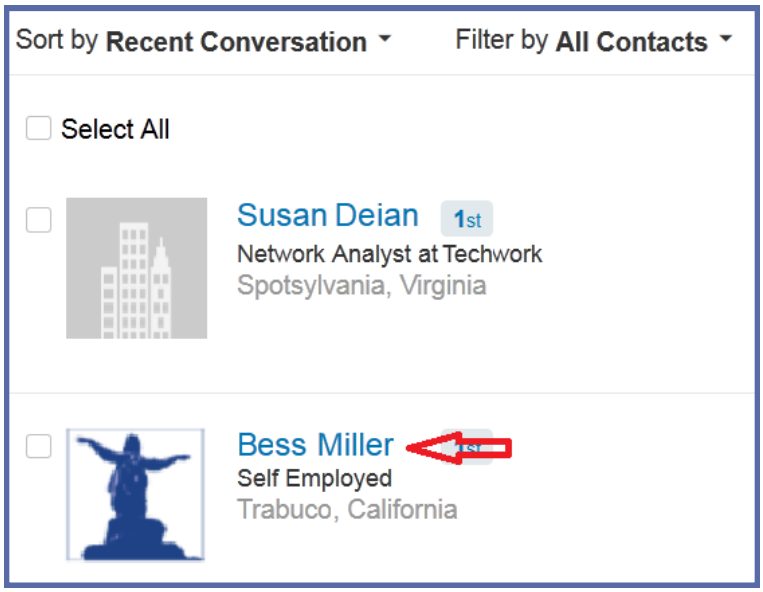
Blocking or Reporting a LinkedIn Member

You can selectively block LinkedIn members from viewing your profile. If you block a user, LinkedIn will not notify the blocked member. If you are connected to them then that connection will be broken. If either has endorsed the other, then those endorsements will be deleted. Neither will be able to view the other's profile and neither can exchange LinkedIn messages with the other.

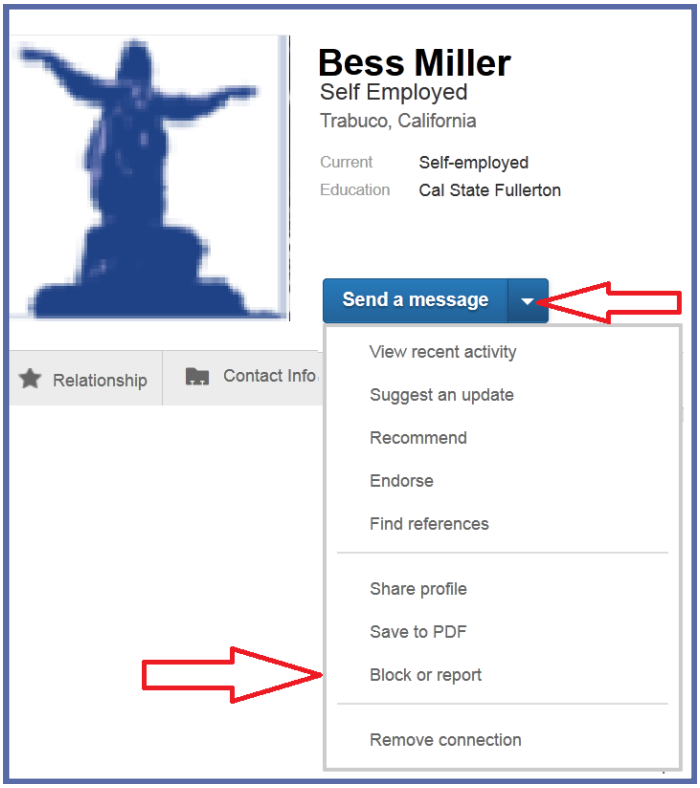
You cannot block anyone from information you have on your public profile or from information you have posted in open groups. Nor can you block a member from commenting on any post you have made in a public discussion group. Mutual connections can share your information with members whom you have blocked.



1. Along the command strip, click **Connections**.

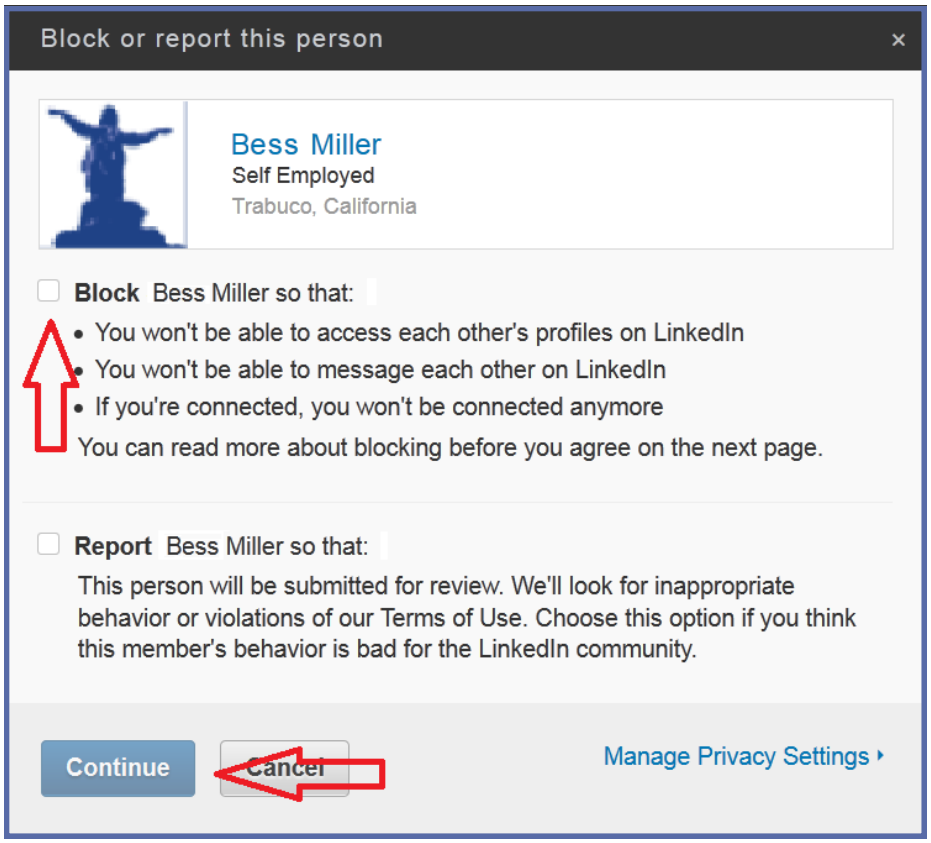


2. Click on the profile name of the person you want to block.

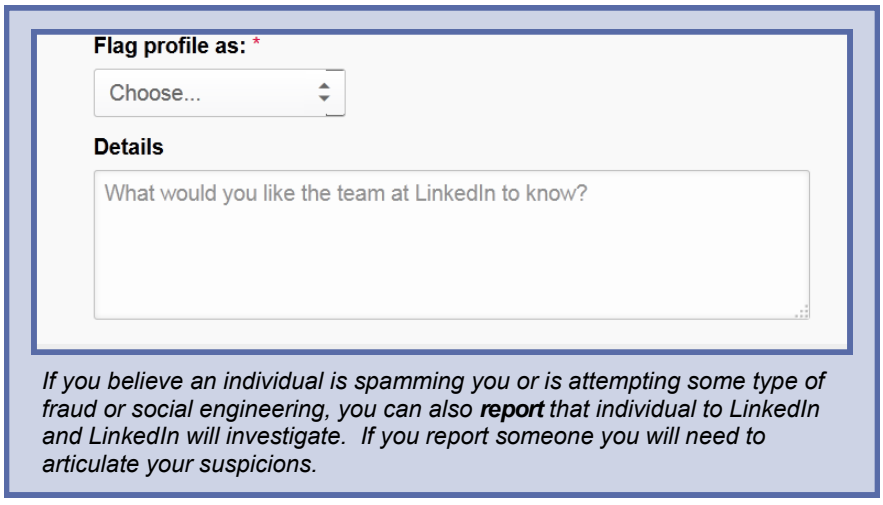


3. Click on the down arrow to the right of **Send a message.**
4. Click **Block or report**.

Cyber Crime Prevention Flyer



5. Click the box next to **Block**.
6. Click **Continue**.



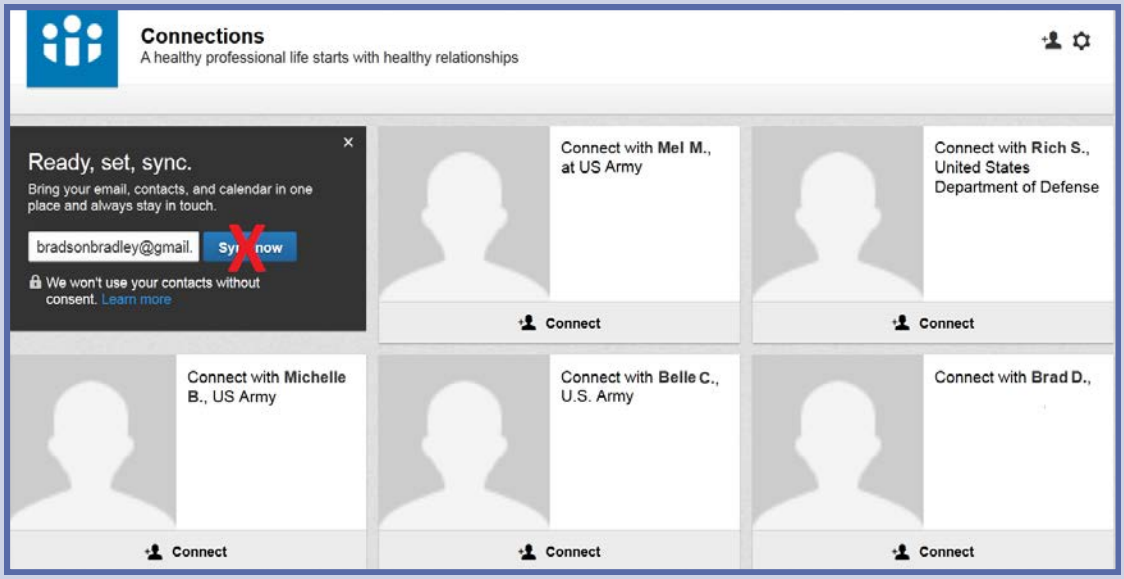
*If you believe an individual is spamming you or is attempting some type of fraud or social engineering, you can also **report** that individual to LinkedIn and LinkedIn will investigate. If you report someone you will need to articulate your suspicions.*

Cyber Crime Prevention Flyer

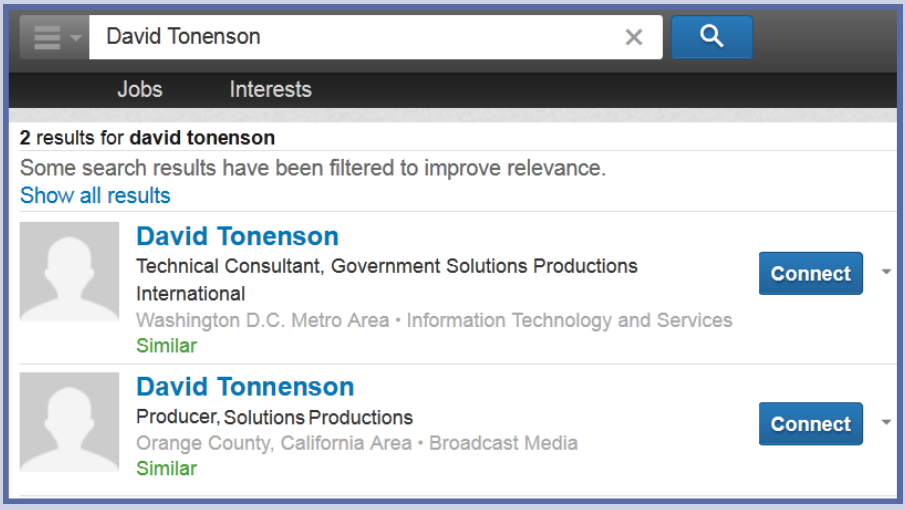
Requesting a Connection

This section shows the multiple means by which you can locate new connections and demonstrates the advanced search features of LinkedIn.

Finding connections is easy because LinkedIn provides several different ways to locate people and, often without effort on your part, suggests connections. This is important not only because it helps you locate reliable connections but shows how easily others, including untrustworthy individuals, with only minimal information can target people with specific backgrounds, like you.

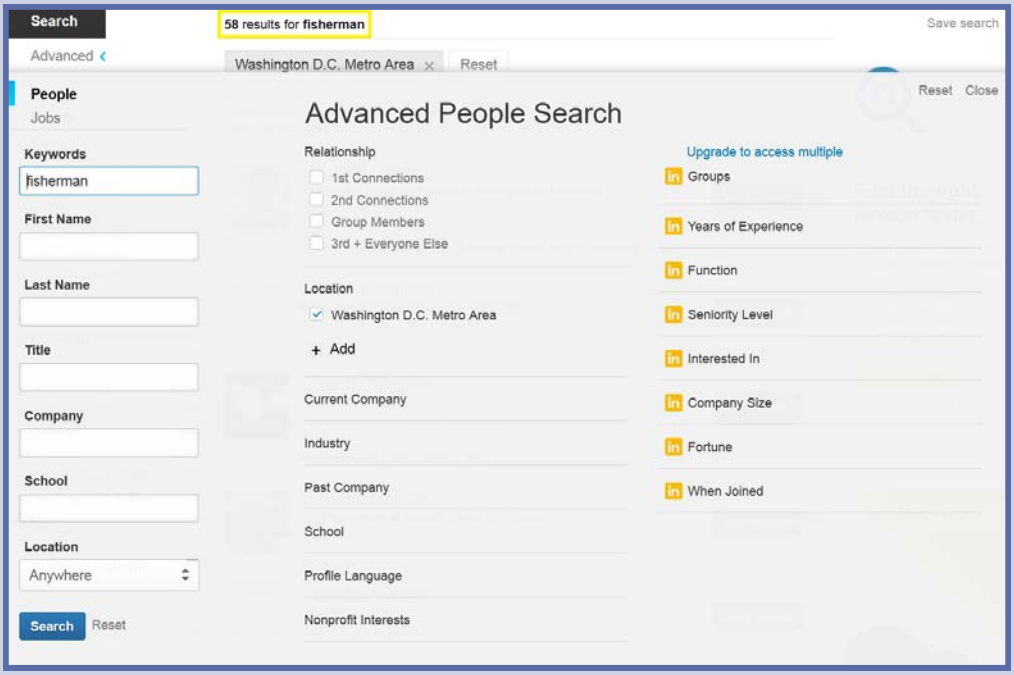


LinkedIn presents opportunities like this to connect with your associates. Note that an invitation to synchronize *your address book is also presented. Resist the temptation.*



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

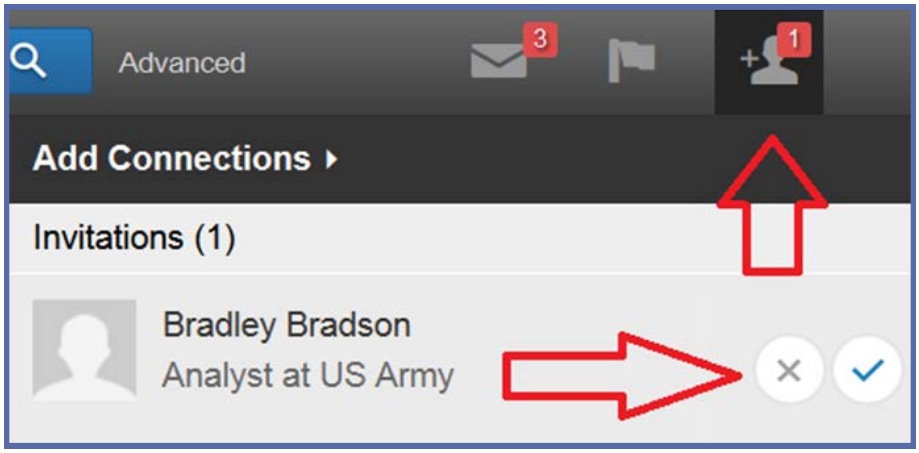
Cyber Crime Prevention Flyer



*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, you will receive a LinkedIn Invitation in your email. The decision to accept or not is important. Your connections are a reflection of your persona.



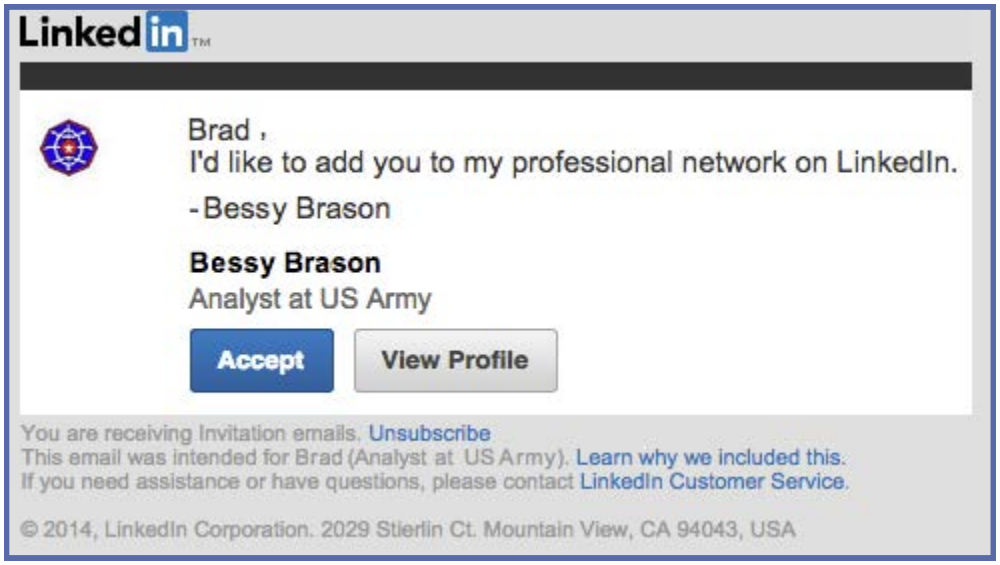
1. Click the blue **check** to accept the invitation or the grey **X** to refuse the invitation.

LinkedIn sends a connection invitation through the LinkedIn site. You will know you have an invitation waiting when you see a red number above the person icon in the command ribbon. Hover your mouse over the red number and a drop down list of pending invitations will appear.

Depending upon your email notification settings, the first indication that a connection request awaits your evaluation might be in your email inbox. Those notifications, however, do not have an **ignore** or **refuse** option. If the connection request is one you want to refuse, the best option is to delete the email, login to your LinkedIn account and refuse the connection request there.

Cyber Crime Prevention Flyer

If you decide to accept the connection request, you can do so from the email in your inbox. However, if you have any concerns about the authenticity of the email, a better option is to login to your LinkedIn account and accept the invitation there.

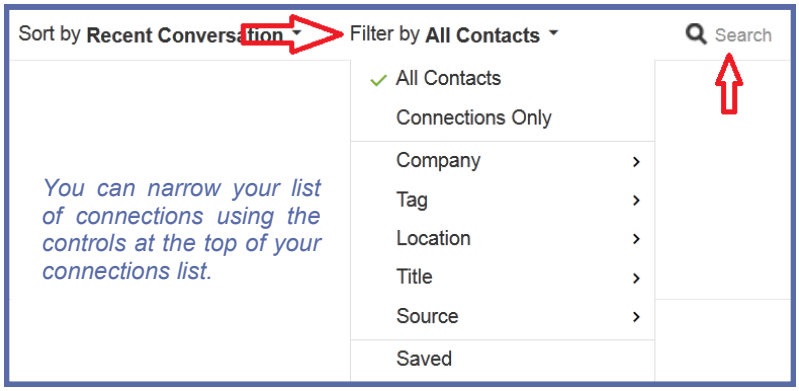


Deleting Existing Connections

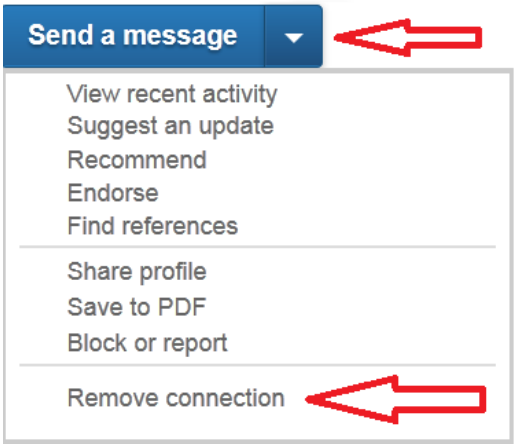
There may come a time when you want or need to remove a connection. When you remove a connection, that person is not notified and only the person breaking the connection can reestablish the connection.

The process to remove a connection is straightforward.

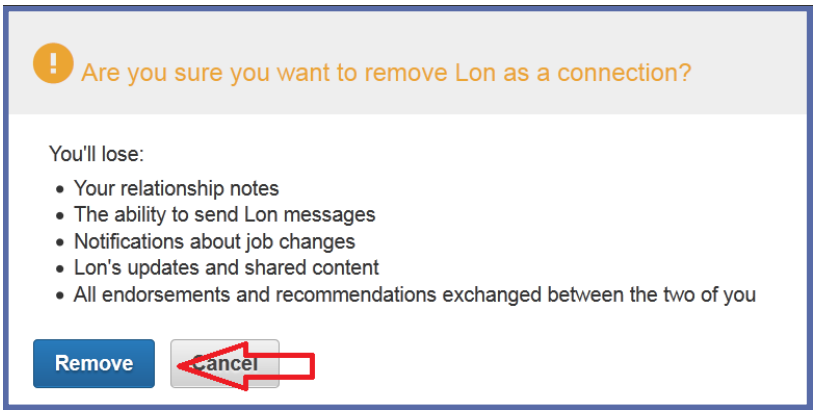
1. Click **Connections** in the command ribbon.
2. Scroll through the list of your connections and click on the name of the connection you want to delete.



3. Once at the connection's profile page, hover your mouse over the **down arrow** to the right of the **Send a message** button then click **Remove connection**.



4. When asked to verify the removal of this connection, click **Remove.**



Endorsement 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. (For more information, 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 made. 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. 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 any of the listed skills to open a second dialog box.

3. Click the **X** by the skill you want to delete.
4. Click **Save**.

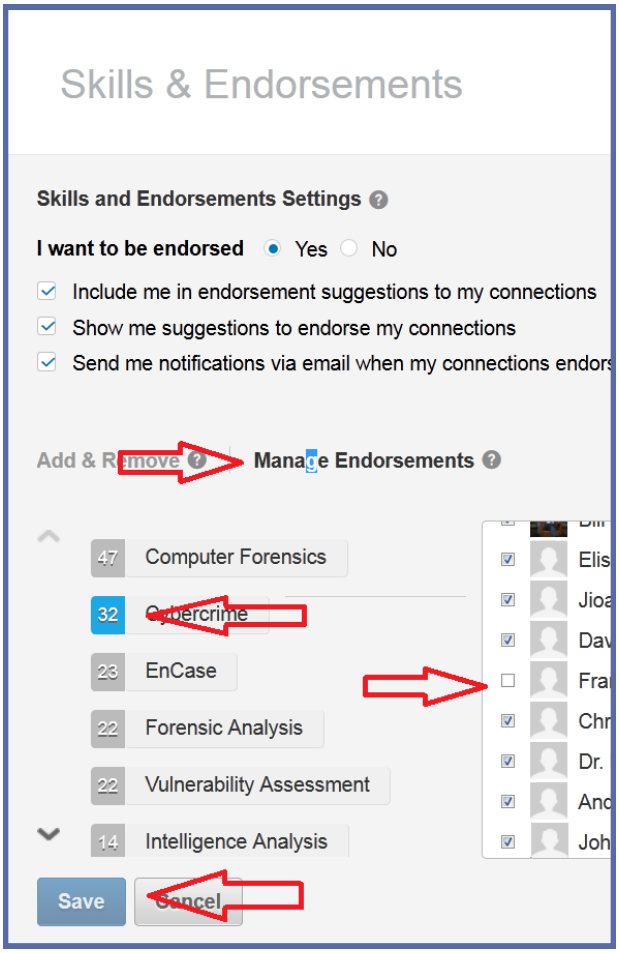
Cyber Crime Prevention Flyer

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.

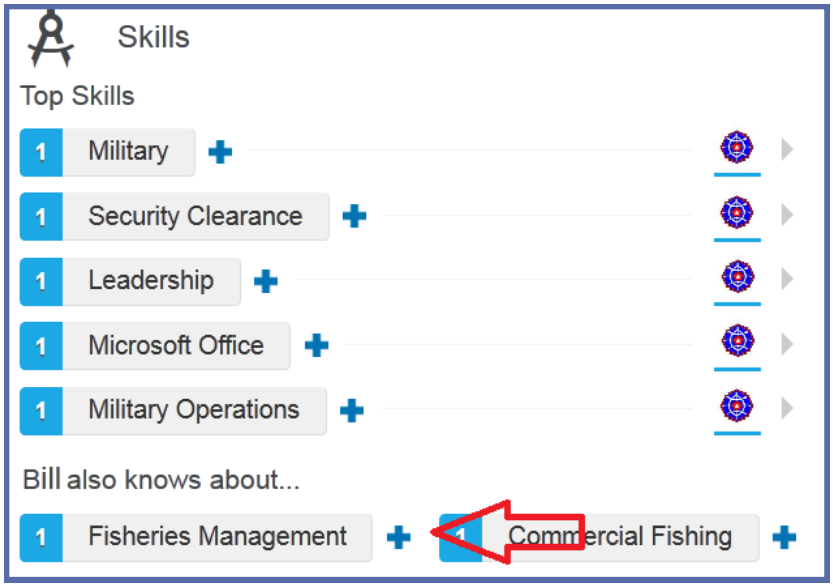
5. Click **Save**.

Cyber Crime Prevention Flyer

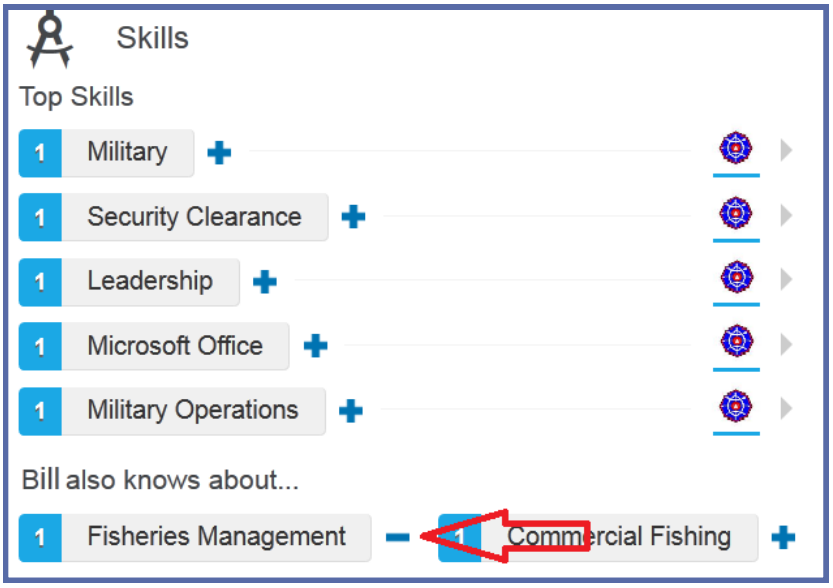
Removing Endorsement You Have Mistakenly Made

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 their 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

Cyber Crime Prevention Flyer

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 a recommendation:

1. Hover your mouse over the upper right corner of the recommendation and click **Manage**.

2. 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.)
3. There is no specific button to confirm this change. Simply navigate away from this page.

Return to **Social Networking Safety Tips**

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