J.P.Morgan

CYBER SAFETY

Securing your social media accounts*

You might be sharing more information about your friends, family and contacts on your social media sites than you realize. This information could be used by fraudsters as part of social engineering efforts. Here are some easy steps to help keep your information more secure across three social media sites.

social media safety guidelines

- Limit the amount of personal information you publish on social media (first dog's name, school, children's names, etc.), as key profile questions can act as answers to vetting questions trying to protect you.
- Report any suspicious activity to the social media site the contact came from. Spam can come in the form of a post, message, email or even a friend request.
- Monitor how your social media sites contact you; they will never ask for personal information through messages, posts or emails.
- Change your password and report the suspicious activity immediately if you think someone has accessed your account.

Facebook

1. Privacy

Limit who can view your activity and personal information on Facebook. Modifying your privacy settings should ensure your information is only seen by those you want.

Facebook offers a feature called **Privacy Checkup,** which allows you to easily review your most important privacy settings and modify them to match your level of risk comfort.

- How to (Desktop only): **Lock** button [in the upper right corner of your screen] > **Privacy Checkup** > [Modify each of the following sections to your level of risk comfort; try to avoid choosing Public]
  - Posts
  - Apps
  - Profile

Further limit who can view your posts and information. Modifying your privacy settings should ensure your information is only seen by those you want.

- How to (Mobile): **More** > **Settings** > **Account Settings** > **Privacy** > [Modify each section below to your level of risk comfort]
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > **Privacy** [on the left side of your screen] > [Modify each section below to your level of risk comfort]

Sections to modify via mobile and desktop access:

- **Who can see my stuff?**
  - Who can see your future posts?
    Suggestion: Friends
- **Who can contact me?**
  - Who can send you friend requests?
    Suggestion: Friends of friends
- **Who can look me up?**
  - Who can look you up using the email address you provided?
    Suggestion: Friends
  - Who can look you up using the phone number you provided?
    Suggestion: Friends
  - Do you want search engines outside of Facebook to link to your Timeline?
    Suggestion: No

More granularly limit who can see what you have posted or what others have posted to your timeline.

- How to (Mobile): **More** > **Settings** > **Account Settings** > **Timeline and Tagging** > [Modify each section to limit who can view your Timeline or tag you in photos or posts to your level of risk comfort, and avoid choosing Public where applicable]
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > **Timeline and Tagging** [on the left side of your screen] > [Modify each Timeline permission to your level of risk comfort, and avoid choosing Everyone where applicable]

Facebook offers a unique service called **Legacy Contact.** Choose a family member or close friend to take care of your account in case of an emergency or if something happens to you.

- How to (Mobile): **More** > **Settings** > **Security** > **Legacy Contact** > [Set up trusted contact and preferences]
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > **Edit** next to Legacy Contact > [Set up trusted contact and preferences]

2. Strengthen your password

A strong password is your front line of defense against unauthorized access to your accounts.

- How to (Mobile): **More** > **Settings** > **Account Settings** > **General** > **Password** > [Enter your current password, then enter your new secure password and confirm] > **Change Password**
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > Click **Edit** next to Password > [Enter your current password, then your new secure password and confirm] > **Save Changes**

3. Two-factor authentication

To ensure an unauthorized person is not attempting to access your account, Facebook can provide you with a security code when you access your account from a new device.

- How to (Mobile): **More** > **Settings** > **Account Settings** > **Security** > Login Approvals: **On** > **Start Setup** > [Follow activation steps]
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > Click **Edit** next to Login Approvals > Check box to enable **Security Code** > **Get Started** > [Follow activation steps] > **Save Changes**

4. Login alerts

Facebook can send notifications, emails or text messages when your account is accessed from a new computer or device.

- How to (Mobile): **More** > **Settings** > **Account Settings** > **Security** > **Login Alerts** > [Choose where you would like to receive alerts]
- How to (Desktop): **Down arrow** [in the upper right corner of your screen] > **Settings** > **Security** [on the left side of your screen] > Click **Edit** next to Login Alerts > [Choose where you would like to receive alerts]

LinkedIn

1. Privacy

Limit who can view your posts and personal information on LinkedIn. Modifying your privacy settings should ensure your information is only seen by those you want.

- How to (Desktop only): **Photo Dropdown** > **Privacy & Settings** > **Privacy Controls** > [Modify each setting to your level of risk comfort]

  Pay special attention to:

  – Select who can see your activity feed
  Suggestion: Your Connections

  – Select who can see your connections
  Suggestion: Only you

Control who can contact you via LinkedIn. Modifying your communication settings will limit who can send you invites and messages.

- How to (Desktop only): **Photo Dropdown** > **Privacy & Settings** > **Communications** > [Modify each setting based on your level of risk comfort]

  Pay special attention to:

  – Select the types of messages you'd prefer to receive
  Suggestion: Introductions Only

  – Select who can send you invitations
  Suggestion: Only people who know your email address or appear in your "Imported Contacts" list

2. Strengthen your password

A strong password is your front line of defense against unauthorized access to your accounts.

- How to (Mobile): Tap **Me** > Tap the **gear icon** > **Change password** > [Enter your current password, then your new secure password and confirm] > **Save**
- How to (Desktop): **Photo Dropdown** > **Privacy & Settings** > Click **Change** next to password [on the left side of your screen] > [Enter your current password, then your new secure password and confirm] > **Change password**

3. Two-factor authentication

To ensure an unauthorized person is not attempting to access your account, LinkedIn can provide you with a security code when you access your account from a new device.

- How to (Desktop only): **Photo Dropdown** > **Privacy & Settings** > **Account** > **Manage security settings** > Two-step verification for sign-in: **Turn On** > [Follow activation steps]

Twitter

1. Privacy

Limit who can view your tweets and personal information on Twitter. Modifying your privacy settings should ensure your information is only seen by those you want.

- How to (Desktop): **Picture Dropdown** > **Settings** > **Security and privacy** > Check the box next to **Protect my Tweets** > **Save changes**
- How to (iOS): Tap **Me** > Tap the **gear icon** > **Settings** > Select account > **Privacy** > Switch Protect my Tweets: **On**
- How to (Android): Tap the **three dots** [in the upper right corner of your screen] > **Settings** > Select account > **Privacy and content** > Check box next to **Protect my Tweets**

2. Strengthen your password

A strong password is your front line of defense against unauthorized access to your accounts.

- How to (Desktop): **Picture Dropdown** > **Settings** > **Password** > [Enter your current password, then your new secure password and confirm] > **Save changes**
- How to (iOS): *For security reasons, changing your Twitter password is disabled on iOS devices*
- How to (Android): Tap the **three dots** [in the upper right corner of your screen] > **Settings** > Select account > **Change Password** > [Enter your current password, then your new secure password and confirm] > **Change Password**

3. Two-factor authentication

To ensure an unauthorized person is not attempting to access your account, Twitter can provide you with a security code when you access your account from a new device.

- How to (Desktop): **Picture Dropdown** > **Settings** > **Security and privacy** > Check **Verify login requests** > [Follow steps to enable] > **Save changes**
- How to (iOS): Tap **Me** > Tap the **gear icon** > **Settings** > Select account > **Security** > Switch Login Verification: **On** > **Confirm**
- How to (Android): Tap the **three dots** [in the upper right corner of your screen] > **Settings** > Select account > **Security** > Check the box next to **Login Verification** > [Follow steps to enable]

 0115-0064-22

CSA-SOCMED-V4-121415