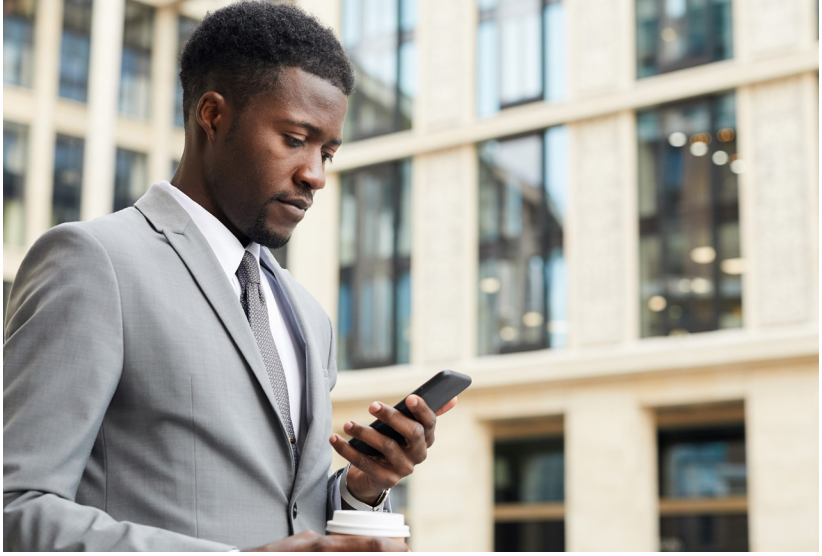

# Use social media wisely: security tips for business users

LinkedIn is a great way to connect professionally with people in your industry. Cybercriminals agree. Hackers gather information about people and companies from public social media profiles. Some set up fake profiles, posing as business associates to connect with people in order to solicit more specific information. Hackers then use that information to craft personalized emails, called spear phishing emails, that appear quite believable. Recipients are more likely to respond to these emails (or click an attachment link that installs malware on their computer or directs them to a malicious website) as they are familiar with the names gathered by the hackers and used in the emails.

## When to accept or not accept invitations.

- To help protect you and your business from spear phishing attempts, don't include any personal information (such as, birthdate) or non-public information about your business on your LinkedIn profile.
- Accept invitations only from people you know in real life or who have been personally verified by people you know; and only send invitations to people you know professionally.
- Consider keeping your professional connections separate from your personal ones. If a business colleague wants to friend you on Facebook, ask to connect through LinkedIn. You can easily remove a connection, or block or report a member on LinkedIn.

usbank

## Strong, unique passwords are key.

Create a separate, strong password or passphrase for each online site that uses confidential data, and change them frequently. If one social media site is breached and hackers get your password; they can't use it to access your information on other sites. A strong password contains capital and lower case letters, numbers and symbols. Don't use common words or personal information for your password. Consider using a password vault, a program that stores user names and passwords in a secure location in an encrypted format, to help you manage your passwords.

## Strengthen your social media security

Add an extra layer of security by using two-factor authentication, in addition to your password or passphrase, on your social media accounts. Most social media sites, including LinkedIn, have this feature. Once it is enabled, LinkedIn sends a one-time code to your mobile device when you log in from a device or browser you haven't used before. You must enter that code to access LinkedIn. To turn on this feature, click your profile icon, select Settings & Privacy, click the Sign in & Security tab, and select Account Access. Under Two-Step Verification, click Turn On, enter your mobile phone number, and click Send Code.

## Watch out for phishing emails.

LinkedIn and other legitimate companies won't ask you for personal information, such as passwords, or make threats in emails.

- Examine all emails carefully for suspicious claims, poor or unprofessional writing, and logos and theme colors that are not quite right.
- Don't click links or attachments in any email message; it's safer to go directly to LinkedIn or any site by typing the URL in your Internet browser.
- Follow these security tips and visit LinkedIn's Safety Center for more LinkedIn privacy and security information.

## Update your privacy settings on LinkedIn

It's best to review and update your privacy settings on LinkedIn every few months since online features are updated frequently. Click your profile picture or icon, and select Settings & Privacy. Click each setting option to read and update, and then click Save Changes. These are some of the privacy options you should adjust:

**Turn on or off your activity broadcasts**
If you don't want your connections to know when you change your profile, recommend connections, or follow companies, uncheck this option.

**Select who can see your activity feed**
Select who can see your actions on LinkedIn. Select "Your connections" for greater privacy than selecting "Everyone."

**Select what others can see when you've viewed their profile**
When you look at other profiles, select whether to display only a general title or to appear as an anonymous LinkedIn member.

**Select who can see your connections**
Select whether to show your connections to your other connections or to keep them visible only to you.

**Change your profile photo and visibility**
Select who can see your photo. Select "Your connections" for greater security than selecting "Everyone."