

# Social Media & LinkedIn Privacy and Security Tips



# Social Media Overview

Social media platforms are a fun way to stay connected on world news, friends and family.

HOWEVER

There are security risks involved when using social media. It's important to secure your accounts and to be careful what and how you post online to protect yourself and the company against cyber-criminal activity.

The work we do is highly valued. Cyber attackers can analyze our social media posts and use them to gain access to the company or into our bank accounts or even our homes. Stay safe online by following social media security best practices.

# Why does social media security matter?



## Phishing and malware attacks

Poor social media security practices can result in an increase in spear phishing attacks against you and the company



## Reputational damage to yourself and the company

Social media security hacks can potentially damage personal and corporate brand reputations.



## Identity theft & financial fraud

Weak or poor social media security practices can result in personal identity and financial fraud.

# Threat: Nation-State threat actors use LinkedIn to identify employees with access to technologies they are seeking to acquire.

COVID-19 has fueled cyber threat activity, because it is cheaper and quicker to steal technology than to develop it independently.

- 1 The COVID-19 crisis has resulted in widespread unemployment of workers in industries being targeted by hostile intelligence agencies, such as tech, aerospace, energy. LinkedIn is used to spot and then establish contact with espionage targets.
- 2 Threat actors use LinkedIn to identify targets to send phishing emails to, steal user credentials, and/or place malware at the company.
- 3 Nation state actors also use LinkedIn as a tool to identify and recruit human sources within target companies to provide information or technology of interest in exchange for money.
- 4 Security budget cuts make companies more vulnerable to hacks — especially if insider threat and cyber security programs are cut just as the threat of corporate espionage involving laid-off employees is increasing.



## RESPONSE

- Increase monitoring and surveillance of phishing attacks.
- Raise staff awareness of social media policy and security best practices through a security awareness campaign.

## KEY LEARNINGS

- Phishing remains the easiest way to break into a corporate network.
- Because of COVID-19, the coming months will be challenging for regular security operations, coupled with the threat of increased corporate espionage threat arising from layoffs.

# Social media best practices

# Social media security best practices

! Limit what you share on social media about your role and work

✓ Follow employee social media guidelines

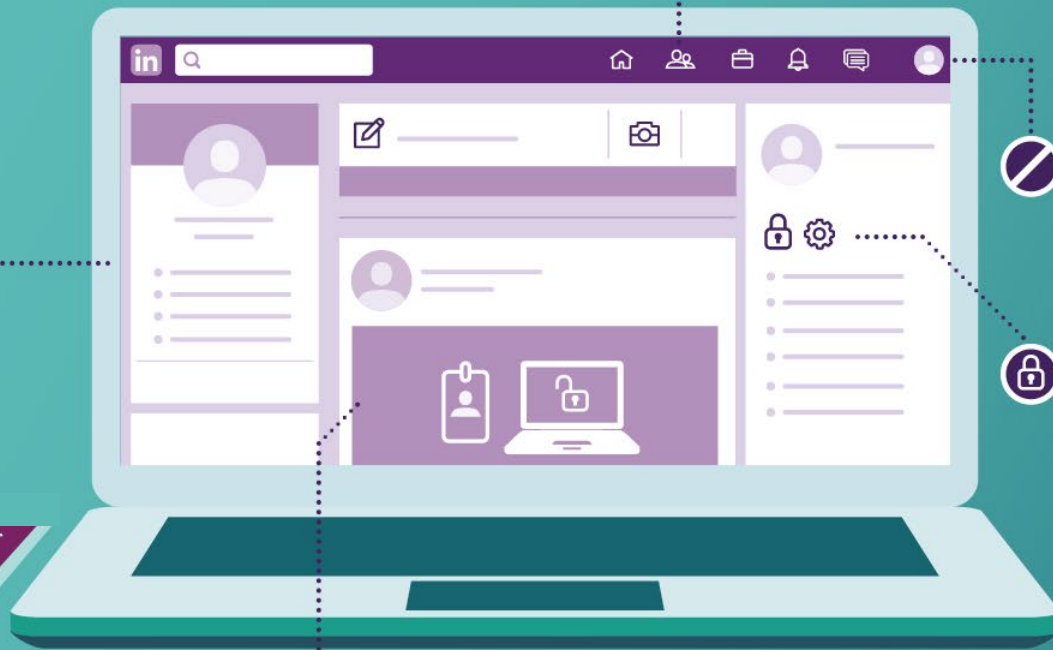


🤝 Don't connect with strangers and watch out for imposter social media profiles

🚫 Don't use your work email and password for social media accounts

🔒 Secure your social media account settings and use two factor authentication

📷 Don't post photos of your work badge or unlocked screen online



# What you can do to stay safe on social media:



**Search** your name on LinkedIn and check for any fake accounts



**Check** [www.haveibeenpwned.com](http://www.haveibeenpwned.com) to see if your credentials have been compromised



**Verify** identities when someone reaches out to you via phone or over the internet

# LinkedIn Tips



# Let's review LinkedIn privacy and security

Social media security  
**best practices**

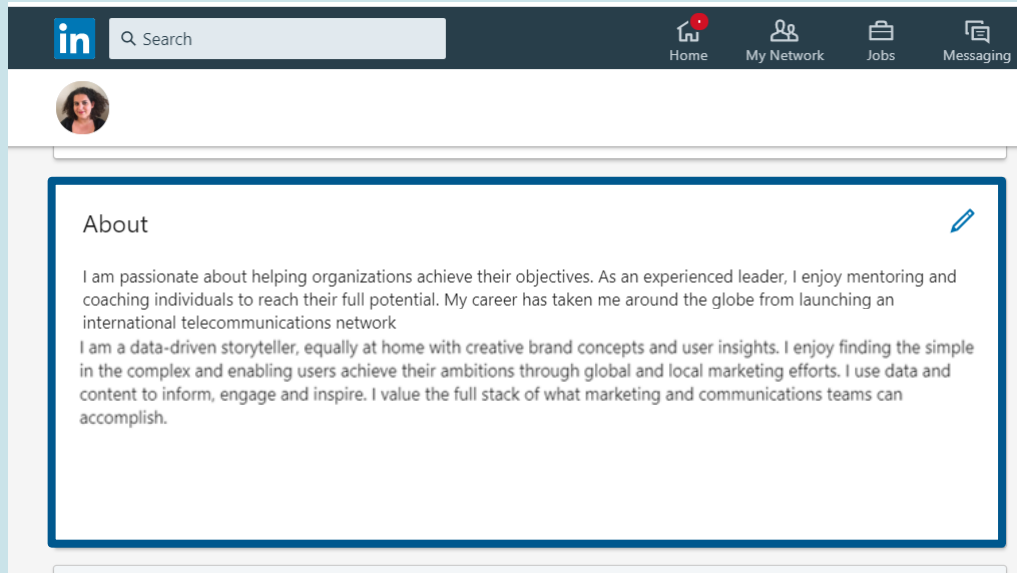


Review your LinkedIn Account  
**Settings & Privacy** to ensure you are  
not oversharing personal details or  
information with third parties.

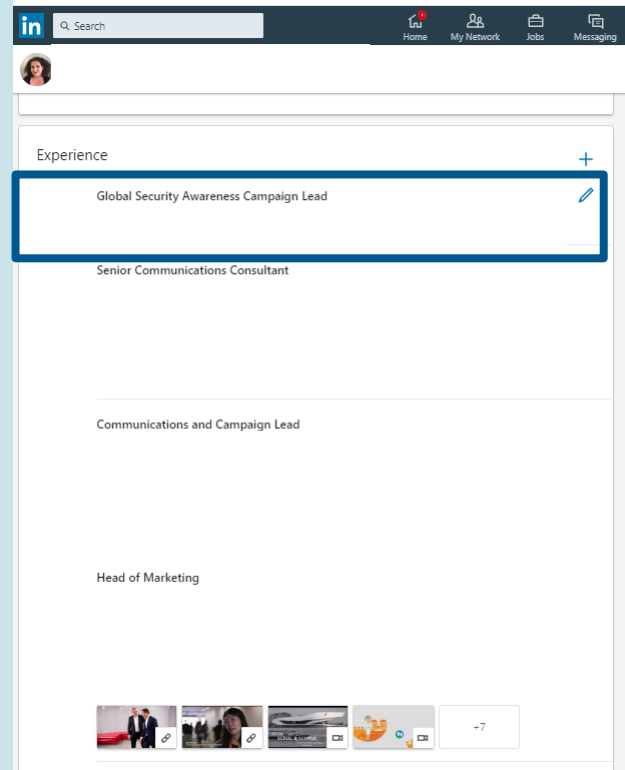
A screenshot of a LinkedIn profile page. The top navigation bar includes the LinkedIn logo, a search bar, and icons for Home, My Network, Jobs, Messaging, Notifications, Me, Work, and Learning. The profile header shows a blue background with a network diagram, a profile picture of a woman, and the text '500+ connections · Contact info'. Below the header, the 'Profile Strength: Intermediate' is displayed. A dropdown menu is open from the profile picture, listing options: 'View profile', 'Try Premium Free for 1 Month', 'ACCOUNT' (with 'Settings &amp; Privacy' highlighted), 'Help', 'Language', 'MANAGE' (with 'Posts &amp; Activity', 'Job posting account', and 'Sign out' listed below), and 'Sign out'. The bottom of the page shows a browser address bar with the URL 'https://www.linkedin.com/psettings/' and a 'Messaging' button.

# Let's review role description

Limit what you share about your role. **Do not share confidential information or project details** in your role description.



The screenshot shows the LinkedIn profile 'About' section. The text is enclosed in a blue border. The text reads: "I am passionate about helping organizations achieve their objectives. As an experienced leader, I enjoy mentoring and coaching individuals to reach their full potential. My career has taken me around the globe from launching an international telecommunications network. I am a data-driven storyteller, equally at home with creative brand concepts and user insights. I enjoy finding the simple in the complex and enabling users achieve their ambitions through global and local marketing efforts. I use data and content to inform, engage and inspire. I value the full stack of what marketing and communications teams can accomplish."



The screenshot shows the LinkedIn profile 'Experience' section. The first role, "Global Security Awareness Campaign Lead", is highlighted with a blue border. Below it are "Senior Communications Consultant", "Communications and Campaign Lead", and "Head of Marketing". The bottom of the page shows a row of four small image thumbnails with edit icons and a "+7" button.

# Let's review LinkedIn security account settings (1 of 2)

The screenshot shows the LinkedIn account settings page. The top navigation bar includes the LinkedIn logo, a 'Back to LinkedIn.com' link, and a user profile picture. Below the navigation bar, there are four main tabs: 'Account', 'Privacy', 'Ads', and 'Communications'. The 'Account' tab is selected and highlighted with a blue underline. On the left side, there is a sidebar menu with the following items: 'Login and security', 'Site preferences' (highlighted with a blue border), 'Subscriptions and payments', 'Partners and services', and 'Account management'. The main content area is divided into several sections, each with a title and a 'Change' link. The sections are: 'Phone numbers' (Add a phone number in case you have trouble signing in, 1 phone number), 'Change password' (Choose a unique password to protect your account, Last changed: November 13, 2016), 'Where you're signed in' (See your active sessions, and sign out if you'd like, 4 active sessions), 'Devices that remember your password' (Review and control the devices that remember your password, 0 devices), and 'Two-step verification' (Activate this feature for enhanced account security, On). The 'Change password' and 'Two-step verification' sections are highlighted with blue borders.

Account Privacy Ads Communications

Account

Site preferences

Change password

Two-step verification

Do not reuse passwords from other accounts. Never use your company email or password for social media accounts. Switch on Two Factor Authentication on your social media accounts.

# Let's review LinkedIn account settings (2 of 2)

The screenshot shows the LinkedIn account settings page. The top navigation bar includes the LinkedIn logo, a 'Back to LinkedIn.com' link, and a user profile picture. The main content area is divided into three tabs: 'Account', 'Privacy', and 'Communications'. The 'Privacy' tab is active and highlighted with a blue border. Under the 'Privacy' tab, there are four main sections: 'How others see your profile and network information', 'How others see your LinkedIn activity', 'How LinkedIn uses your data', and 'Job seeking preferences'. The 'How others see your profile and network information' section is expanded, showing four sub-sections: 'Manage who can discover your profile from your email address', 'Manage who can discover your profile from your phone number', 'Sync contacts', and 'Sync calendar'. Each sub-section has a 'Change' link and a dropdown menu showing the current setting (e.g., 'Nobody').

Account Privacy Ads Communications

Get a copy of your data  
See your options for accessing a copy of your account data, connections, and more.

How others see your profile and network information

How others see your LinkedIn activity

How LinkedIn uses your data

Job seeking preferences

Blocking and hiding

**Manage who can discover your profile from your email address** Change  
Nobody

Choose who can discover your profile if they are not connected to you but have your email address

**Manage who can discover your profile from your phone number** Change  
Nobody

Choose who can discover your profile if they have your phone number

**Sync contacts** Change

Manage or sync contacts to connect with people you know directly from your address book

**Sync calendar** Change

Manage or sync calendar to get timely updates about who you'll be meeting with

Secure your LinkedIn account by restricting visibility of your email and phone number and do not sync contacts or your calendar.

# Let's review LinkedIn account visibility

Back to LinkedIn.com

You control your profile and can limit what is shown on search engines and other off-LinkedIn services. Viewers who aren't signed in to LinkedIn will see all or some portions of the profile view displayed below.

[Sign in to Connect](#)

**Edit your custom URL**  
Personalize the URL for your profile.  
www.linkedin.com/in/shereehanafi

**Edit Content**  
This is your public profile. To edit its sections, update your profile.  
[Edit contents](#)

**Edit Visibility**  
You control your profile's appearance for people who are not signed in to LinkedIn. The limits you set here affect how your profile appears on search engines, profile badges, and permitted services like Outlook.  
[Learn more](#)

Your profile's public visibility On

Check your profile visibility to connections outside of your network. LinkedIn has a variety of options to enable you to restrict what you share.

Back to LinkedIn.com

You control your profile and can limit what is shown on search engines and other off-LinkedIn services. Viewers who aren't signed in to LinkedIn will see all or some portions of the profile view displayed below.

**Edit Content**  
This is your public profile. To edit its sections, update your profile.  
[Edit contents](#)

**Edit Visibility**  
You control your profile's appearance for people who are not signed in to LinkedIn. The limits you set here affect how your profile appears on search engines, profile badges, and permitted services like Outlook.  
[Learn more](#)

**Your profile's public visibility** On

**Basic (required)**  
 Name, number of connections, and region

**Profile Photo**  
 Only 1st degree connections  
LinkedIn members directly connected to you.  
 Your network  
Your connections, up to three degrees away from you.  
 All LinkedIn members

Public  
All LinkedIn members on or off LinkedIn. Your content could be visible in search results (Google, Bing, etc.).

**Headline** Show   
**Summary** Show   
**Articles & Activity** Hide   
**Current Experience** Hide   
**Past Experience** Hide   
**Education** Hide   
**Projects** Hide   
**Languages** Hide   
**Groups** Hide   
**Recommendations** Hide

**Public Profile badge**  
Promote your profile by adding a badge to your blog, online resume, or website.