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
- 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
- Follow employee social media guidelines
- 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

Review your LinkedIn Account Settings & Privacy to ensure you are not oversharing personal details or information with third parties.
Let's review role description

Limit what you share about your role. **Do not share confidential information or project details** in your role description.
Let’s review LinkedIn security account settings (1 of 2)

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)

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Change Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage who can discover your profile from your email address</td>
<td>Nobody</td>
</tr>
<tr>
<td>Manage who can discover your profile from your phone number</td>
<td>Nobody</td>
</tr>
<tr>
<td>Sync contacts</td>
<td>Change</td>
</tr>
<tr>
<td>Sync calendar</td>
<td>Change</td>
</tr>
</tbody>
</table>

Manage who can discover your profile from your email address:
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:
Choose who can discover your profile if they have your phone number.

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

Sync calendar:
Manage or sync calendar to get timely updates about who you’ll be meeting with.
Let’s review LinkedIn account visibility

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