



NordLayer®

77% organizations from
small to large have a
LinkedIn profile

LinkedIn scams report



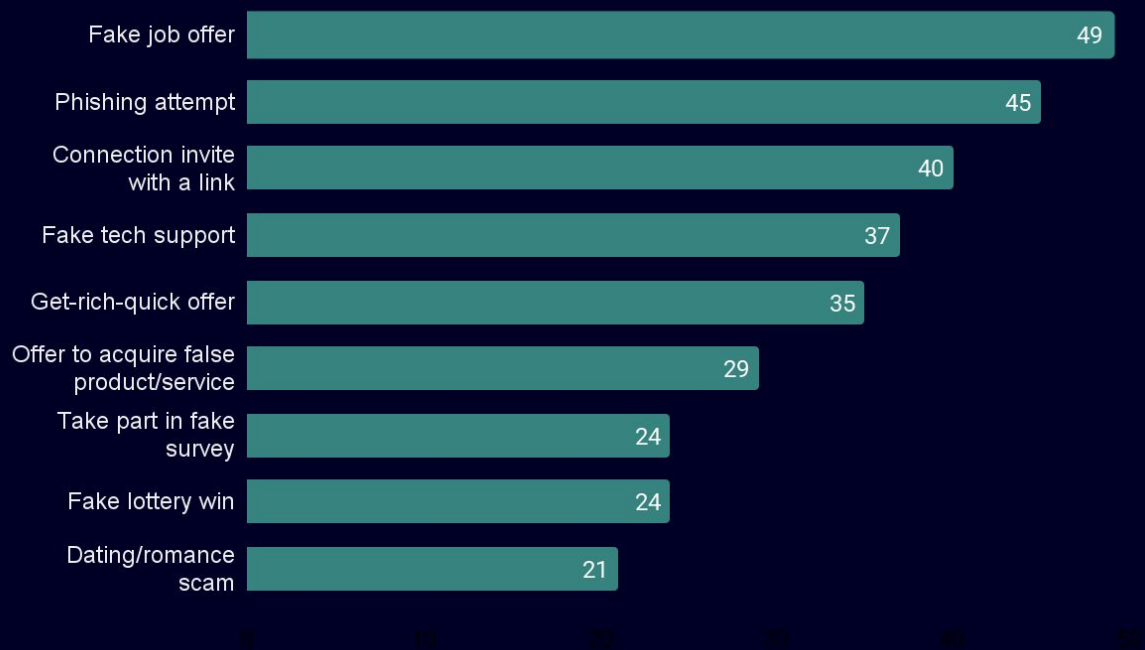
The methodology

- NordLayer surveyed 500 companies (non-governmental organizations) in Canada, the United Kingdom, and the United States.
- Subindustries: business management & support services, e-commerce, education, finance & insurance, health care, information and communication, IT, professional & technical services, and consulting.
- Company size
 - Small: 1-10 employees
 - Medium: 11-200 employees
 - Large: 201+ employees

LinkedIn scam

It is a fraudulent scheme on the LinkedIn platform that aims to trick people into giving money or personal information, often through a fake job or business opportunities, requests for payment, or impersonation.

Typical LinkedIn scams



LinkedIn, a professional networking platform, is an attractive target for scammers exploiting its career-building focus.

Common scams include fake job offers to collect personal info or money, phishing through impersonation, exploiting the connection culture to spread malicious content, or using social engineering based on public or personal data.

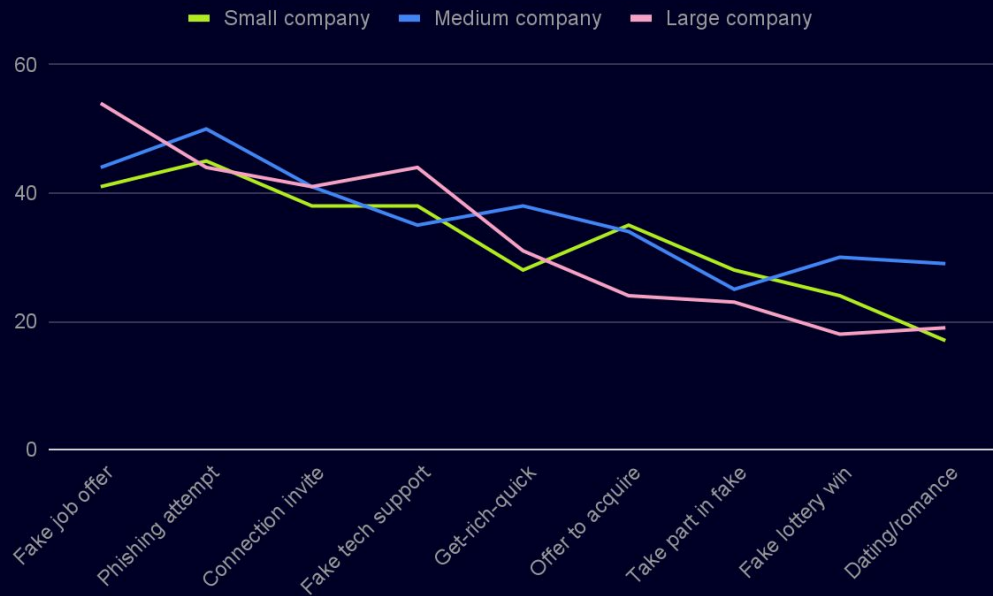
Fake professional persona on LinkedIn can create a "smoke screen," leading to unexpected scams, including lotteries or romance fraud.

Fake job offers is the
most encountered scam
type in the United
Kingdom



LinkedIn scam trends by company size

According to the research, over half of the respondents encountered a scam attempt or fake account on LinkedIn.



Small companies experience less scam activity on LinkedIn, with 52% reporting no such experiences.

47% of respondents note their organization's employees are likely to encounter a scam, particularly those with advanced cybersecurity maturity.

Despite having higher cyber awareness, larger and mature companies fall victim to phishing and fake tech support scams due to outsourced assets and extensive networks.

Mid-sized businesses encounter more offers for non-existent products or services, fake lotteries, and dating/romance scams than their smaller and larger counterparts.




Research data distribution is fairly even across different countries, with the highest LinkedIn activity in the US, followed by the UK and Canada.

Scam engagement is lower in the US compared to the other two. Fake job offers and get-rich-quick scams primarily target the UK.

The US experiences more requests to connect with suspicious links and fake survey invitations. At the same time, scams in Canada tend to involve offers to buy non-existent products or services and dating/romance frauds.

Phishing attempts and fake tech support scams have almost equal distribution across all countries.

Fraud tendencies among countries

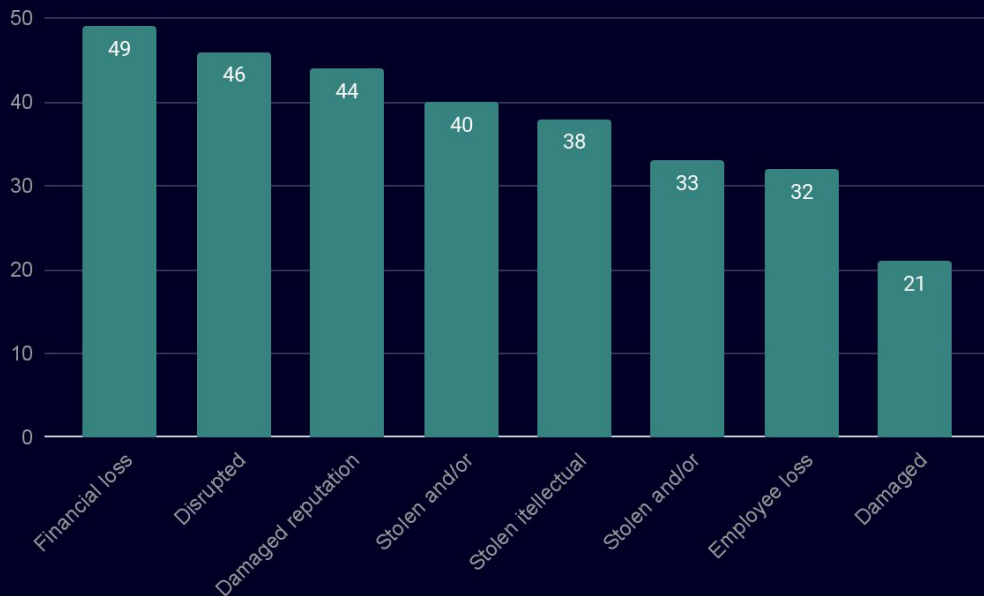
	 Canada	 The UK	 The US
Fake job offer	41%	63%	41%
Phishing attempt	47%	47%	46%
Connection invite with a link	38%	37%	47%
Fake tech support	38%	38%	37%
Get-rich-quick offer	29%	43%	31%
Offer to acquire false product/service	36%	19%	30%
Take part in fake survey	25%	18%	30%
Fake lottery win	24%	19%	30%
Dating/romance scam	30%	15%	23%

67% of small businesses
experience financial loss
after falling victim to
LinkedIn scam



Aftereffects of LinkedIn scams

Half of the organizations surveyed had their reputation damaged.



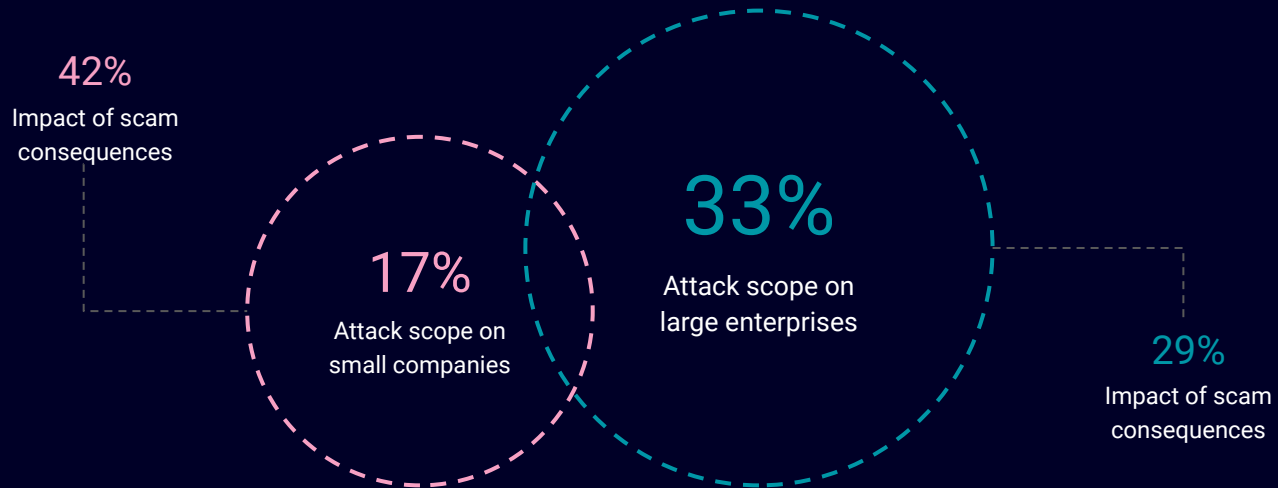
Small businesses bear the brunt of cyber attacks, with significant impacts including financial loss (67%), stolen intellectual property, operation disruption (58% each), and reputational damage.

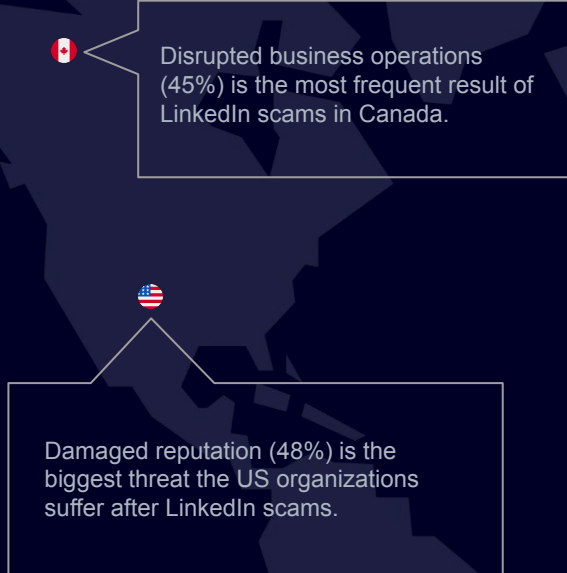
The attacks result in higher employee attrition rates (42%) in small businesses compared to medium and large enterprises (16% and 22%, respectively).

Medium-sized enterprises face the most reputational damage (47%), data theft or damage, and loss of customer contacts (43% each). They are also uniquely prone to infrastructure damage (25%) compared to other business sizes.

Scope of attacks & consequences on small and large enterprises

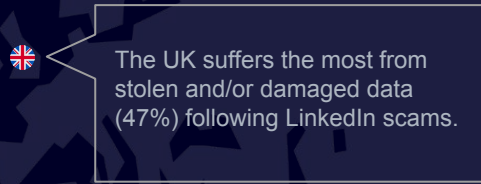
Although small-sized businesses get attacked less than large organizations, the scope of the attack is more impactful.





Disrupted business operations (45%) is the most frequent result of LinkedIn scams in Canada.

Damaged reputation (48%) is the biggest threat the US organizations suffer after LinkedIn scams.



The UK suffers the most from stolen and/or damaged data (47%) following LinkedIn scams.

Recognizing Fake LinkedIn Profiles

- Check links in the profile. Be wary of shortened or redirecting links.
- Look for inconsistencies or lack of detail in the profile, like minimal information or no profile picture.
- Investigate profile activity. Low engagement or mass connection requests can indicate fake accounts.
- Beware of suspicious or irrelevant job offers, promotions, or messages.

For complete report on B2B LinkedIn scams, please see [here](#).