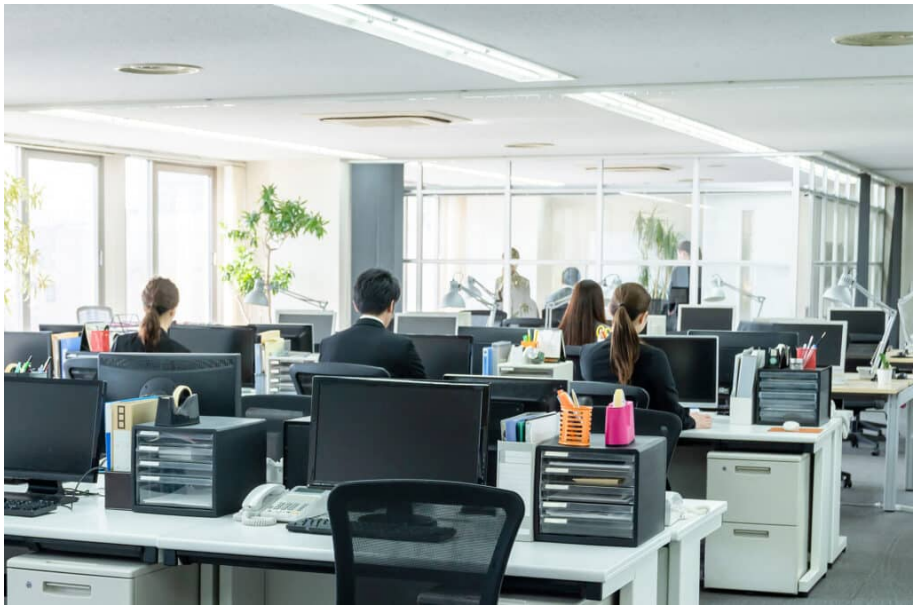
FMBusinessDaily

44% of British businesses subject to Linkedin scams

3 years ago



Nearly half of businesses in the UK (44%) have experienced at least one LinkedIn scam this year, according to the newest research by NordLayer, a network security solution provider.

The most affected tend to be big companies (65%), fake job offers are the most popular scam they encounter (63%), and damaged reputation, as well as stolen/damaged data (47% each) were the leading outcomes of LinkedIn scams.

“Like in every social media platform, attackers and scammers seek information and money or ruin reputations. We know that employees are considered to be the weakest link in the cybersecurity chain, and LinkedIn has millions of professional accounts, making it an even more appealing target for scammers. So no one should let their guard down, no matter how professional a message might look,” said cybersecurity expert Carlos Salas.

What size companies are the most affected by LinkedIn scams?

According to the research, 65% of big companies have been contacted by a scam/fake account on LinkedIn at least once. Furthermore, 58% of medium and 31% of small companies have experienced it at least once.

Mr Salas said: “Cyberattacks are a major threat to businesses of all sizes. However, big companies are often the most targeted due to their data and value. They also have larger networks and databases, making them vulnerable to attack if their security measures are not up to par. Hackers will often focus their efforts on these targets to maximize their rewards.”

Most common types of LinkedIn scams and employees' response to them

Data revealed that fake job offers (63%) is the most prevailing LinkedIn scam among British businesses. Moreover, they also experience active phishing attempts (47%), get-rich-quick offers (43%), and fake tech support (38%).

Surprisingly, 50% of UK companies are also aware of a scam on LinkedIn using their organization's brand name. This type of scam was the most prevalent among big companies (53%), but it's also common among smaller ones: 53% of these businesses indicated that this type of scam also happened to them. Only small companies noted that they almost never experience such scams (13%).

Research also shows that the most popular employee action against these scams in the UK was to inform the community about it with a post on social media (68%). Employees were also eager to contact LinkedIn administrators (66%) as well as distribute a press piece for journalists informing them about the incident (57%).

Damaged reputation is the leading outcome of LinkedIn scams for big organizations

As the leading outcome of LinkedIn scams, UK companies named damaged reputation as well as stolen/damaged data (47% each) and high financial loss (43%). Moreover, they also experienced stolen/damaged client contacts (41%) and interruption to operations (36%).

Nearly half of businesses in the UK (44%) have experienced at least one LinkedIn scam this year, according to the newest research by NordLayer, a network security solution provider.

The most affected tend to be big companies (65%), fake job offers are the most popular scam they encounter (63%), and damaged reputation, as well as stolen/damaged data (47% each) were the leading outcomes of LinkedIn scams.

"Like in every social media platform, attackers and scammers seek information and money or ruin reputations. We know that employees are considered to be the weakest link in the cybersecurity chain, and LinkedIn has millions of professional accounts, making it an even more appealing target for scammers. So no one should let their guard down, no matter how professional a message might look," said cybersecurity expert Carlos Salas.

What size companies are the most affected by LinkedIn scams?

According to the research, 65% of big companies have been contacted by a scam/fake account on LinkedIn at least once. Furthermore, 58% of medium and 31% of small companies have experienced it at least once.

Mr Salas said: "Cyberattacks are a major threat to businesses of all sizes. However, big companies are often the most targeted due to their data and value. They also have larger networks and databases, making them vulnerable to attack if their security measures are not up to par. Hackers will often focus their efforts on these targets to maximize their rewards."

Most common types of LinkedIn scams and employees' response to them

Data revealed that fake job offers (63%) is the most prevailing LinkedIn scam among British businesses.

Moreover, they also experience active phishing attempts (47%), get-rich-quick offers (43%), and fake tech support (38%).

Surprisingly, 50% of UK companies are also aware of a scam on LinkedIn using their organization's brand name. This type of scam was the most prevalent among big companies (53%), but it's also common among smaller ones: 53% of these businesses indicated that this type of scam also happened to them. Only small companies noted that they almost never experience such scams (13%).

Research also shows that the most popular employee action against these scams in the UK was to inform the community about it with a post on social media (68%). Employees were also eager to contact LinkedIn administrators (66%) as well as distribute a press piece for journalists informing them about the incident (57%).

Damaged reputation is the leading outcome of LinkedIn scams for big organizations

As the leading outcome of LinkedIn scams, UK companies named damaged reputation as well as stolen/damaged data (47% each) and high financial loss (43%). Moreover, they also experienced stolen/damaged client contacts (41%) and interruption to operations (36%).

Image: Shutterstock