UK at risk

of cyber attacks

By Indusface

Recent research has shown that 68% of high-revenue growth companies have embraced a hybrid model worldwide. With businesses enjoying remote or hybrid working, benefits including reduced maintenance costs, improved flexibility and extended talent pool, cyber security awareness has become more critical than ever.

With this in mind, Indusface, a global SaaS company which has undertaken this research, is intrigued to find out the most secure countries for businesses to allow their employees to work from, by creating an index score based on cybersecurity data including DDOS attacks (which stands for Distributed Denial-of-Service, where the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites), phishing sites, Malware hosting sites and compromised computers. Venky Sundar, Founder and President of Indusface also provided six tips for small businesses on ensuring cyber security.

Key Findings

- Finland and Belgium are named the most cyber secure European countries for businesses to allow their employees to work from, with a cyber security index score of 82.45 out of 100.
- The UK is only ranked 12th most cyber secure country in Europe and 40th in the world, with a cyber security score of just 71.19.
- The least cyber secure country is Bulgaria with an index score of 51.92/100.

UK ranked 12th as the most cyber secure European country

Indusface found out that the United Kingdom only ranked 12th in the most cyber secure European countries and the 40th in the global ranking, with an overall cyber security index score of 71.19/100! The UK has an average of 680 phishing sites and 750 malware hosting sites per 100,000 urls, meaning that the chances of sites being fake or containing malware could be high.

Finland received the second-lowest number of DDOS attacks (79) from 2015 to 2021, only 29 attacks higher than France, which has the lowest among the top 10 European countries. This is an important factor for businesses to consider as successful DDOS attacks could block your business sites and bring down all servers and connections you depend on.

Contributing to Belgium's top ranking is that it has the lowest number of compromised computers per 100,000 internet

Top 10 most cyber secure European countries to work from

Rank	Country	DDOS attacks per 100,000 Internet Users	Phishing sites per 100,000 urls	Malware hosting sites per 100,000 urls	Compromised computers per 100,000 internet users	Cyber security index score (/100)
= 1	Finland	79	320	430	47	82.45
= 1	Belgium	314	280	390	11	82.45
3	Austria	175	260	340	137	80.59
4	Switzerland	203	460	470	17	78.09
= 5	Sweden	94	410	390	736	76.31
= 5	Greece	386	370	440	25	76.31
7	Norway	475	340	490	14	75.51
8	France	50	610	850	31	74.92
= 9	Germany	177	480	570	75	73.89
= 9	Estonia	698	540	440	14	73.89

*** Total DDOS Attacks were counted between 2015 to 2021.**
****Compromised computers = have been infected with the Gamarue botnet. Please see full methodology below**
Indusface found out that Finland and Belgium share the title of the most secure European countries for businesses to allow employees to work remotely, each with a cyber security score of 82.45 out of 100.

users (11) in the country. Computers that have been infected with the Gamarue botnet open doors to hackers and make it easier for them to take control of your business data and devices. Belgium also has the joint second lowest malware hosting sites among all top 10 European countries, with an average of 390 sites per 100,000 urls.

Ranking third as the most cyber-secure European country is Austria, with an overall cyber security index score of 80.59/100.

Boasting the lowest number of both malware hosting sites (34) and phishing sites (260) per 100,000 urls, the country owns fewer sites that could trick you or contain malware, making businesses less worried about sensitive information being stolen.

In fourth place is Switzerland with a cyber secure index score of 78.09/100. Sweden and Greece rank joint fifth place with a score of 76.31/100.

Bulgaria ranks the least secure European country for businesses that allow working remotely, with a total cyber security score of only 51.82 out of 100. With 1,220 phishing sites and 1,170 malware hosting sites per 100,000 urls, businesses in the country will need to be extra careful when identifying whether a website is genuine.

Serbia owns one of the highest number of compromised computers per 100,000 internet users (1,467) which leads to its low cyber security score of 53.83 - ranking as the second least cyber-secure European country.

5 least cyber-secure European countries to work from

Rank	Country	DDOS attacks per 100,000 Internet Users	Phishing sites per 100,000 urls	Malware hosting sites per 100,000 urls	Compromised computers per 100,000 internet users	Cyber security index score (/100)
1	Bulgaria	167.40	1220	1,170	430	51.82
2	Serbia	173.61	780	790	1,467	53.83
3	Lithuania	560.74	1010	840	38	55.77
4	Romania	118.00	1040	720	1,435	56.01
5	Croatia	724.60	750	340	2,105	56.57

Venky Sundar, Founder and President of Indusface comments on working remotely across the world:

"Attracting top talent through remote work can revolutionise your business. However, it also leaves your sensitive data and assets vulnerable to hackers. Therefore, it is important to be prepared to address remote work security risks. There are a few points when recruiting talents globally:

Firstly, you could consider which countries are least targeted by hackers and least risk to your cyber security. It's worth looking at regulations that govern data security. For example, GDPR is probably the gold standard when it comes to data security. Research law enforcement. This indicates how quickly people will be punished when committing cybercrime. Get to know the government grants. Cybersecurity grants are provided to SMBs who tend to be more susceptible to attacks.

"Finally, the level of cybersecurity awareness in the generation also affects how likely hackers would commit cyber crimes."

6 top tips for businesses who apply remote or hybrid working

"There is no one way to secure remote working but instead you should make remote work access security an integral part of your employee's ongoing training and workplace culture. Here are six best practices for secure remote working within your business:

1. Create strong authentication

It starts by identifying the remote worker before a worker can access corporate data and assets. From this, you can build audit trails of the actions against the identity.

2. Update your systems and encrypt your devices

Outdated technology could open doors to hackers with credential information like credit cards being stolen. Cases like this will have a fatal hit on your business's reputation as well as cyber security. It is highly recommended that all your devices be updated and encrypted with SSL certificates.

3. Conquer internal security risks

Working habits could lead to malware or ransomware attacks that could put your company and your clients at risk. We recommend hosting full employee training on cyber-security and making it fun. You could get your team engaged in the training by setting up phishing email simulators so they could see the potential dangers in action.

4. Avoid weak or duplicate passwords

Many businesses share duplicate passwords for multiple accounts. Research shows hackers rely on weak passwords when brute forcing PoS terminals. Use an automatic password generator to create safe and secure passwords companywide.

5. Only upload files to secure systems

Hackers could upload their own files with malicious code that can be executed directly on your server. Therefore, it is important to avoid storing data in unencrypted storage, leaving data on devices without password protection, and attaching sensitive information directly into an email.

6. Secure web application security

Using a combination of open-source CMS and cloud-based apps increases your remote work risks. It should be considered as part of your security policy to approve web app purchases and free downloads.

For more information visit: www.indusface.com