Checklist on cybersecurity in international e-commerce.

Cybersecurity is an essential factor to consider in international e-commerce. This is because international e-commerce transactions often involve transferring sensitive data, such as financial and personal data, across borders.

To ensure the safety and security of this data, organizations must employ various security measures, such as encryption, secure payment gateways, and two-factor authentication.

In addition, organizations should also ensure that their websites comply with international privacy and data security laws.

Organizations should monitor their networks for suspicious activity and take appropriate measures to protect against cyber threats.

This tool is designed to let users know whether their international e-commerce business has basic cyber-attack protection measures in place. Large companies often have departments dedicated to these functions, but small companies often need more resources to do so.

This tool will give you a comprehensive overview of how well-protected your business is against cybercrime and perhaps identify gaps or vulnerabilities that can be addressed.

In any case, the user will become aware of aspects of cybersecurity that may not have been considered and is in time to deal with, either personally or through specialised professionals.

Co-funded by the European Union

The tool is a checklist with questions related to cybersecurity and international e-commerce. For each question, there are three possible answers depending on the user's experience:

YES: 

NO: 

I DON'T KNOW: 

Suppose most of the answers are NO or I DON'T KNOW. In that case, we encourage the user to get down to work to improve the security of their international e-commerce business to avoid being a victim of attacks that could lead to large losses or even business failure.

After the checklist, the users will find a series of practical tips on cybersecurity that will guide them on the next steps to take to improve the online security of their international business.

Co-funded by the European Union

E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

CHECKLIST:

Questions			
Is your e-commerce website properly encrypted to protect customer information during transactions?	☐	☐	☐
Have you implemented strong password policies for your customer and administrative accounts?	☐	☐	☐
Do you regularly update your website software and security patches to protect against known vulnerabilities?	☐	☐	☐
Do you have a plan in place to respond to a potential security breach, such as an incident response plan?	☐	☐	☐
Are all risks taken into account in the corporate planning? If not, which one not?	☐	☐	☐
Have you trained your employees on cybersecurity best practices, such as how to spot and prevent phishing attacks?	☐	☐	☐
Do you use secure payment gateways and follow industry-standard security protocols for handling and transmitting sensitive customer information?	☐	☐	☐
Do you have measures in place to detect and prevent unauthorized access to your website and customer data?	☐	☐	☐
Have you conducted regular security assessments and penetration testing to identify and address potential vulnerabilities in your e-commerce system?	☐	☐	☐
Do you have policies and procedures in place for securely disposing of sensitive customer information when it is no longer needed?	☐	☐	☐
Do you have a process for regularly monitoring and reviewing your security measures to ensure they remain effective?	☐	☐	☐

Co-funded by the European Union

Tips on cybersecurity in international e-commerce

1. Use secure networks: Make sure to use secure networks, such as Virtual Private Networks (VPNs), to protect your data while conducting e-commerce transactions.

2. Use strong and unique passwords: Use strong, unique passwords for all of your online accounts and avoid using the same password for multiple accounts.

3. Enable two-factor authentication: Two-factor authentication adds an extra layer of security to your online accounts by requiring you to enter a one-time code in addition to your password.

4. Keep software and systems up to date: Regularly update your software and systems to ensure that you have the latest security patches and features.

5. Use secure payment methods: When conducting e-commerce transactions, use secure payment methods, such as encrypted credit card payments or digital payment systems like PayPal.

6. Be cautious of phishing attacks: Be cautious of phishing attacks, which are attempts to trick you into giving away sensitive information, such as your password or credit card details.

7. Use a reputable security software: Use reputable security software to protect your devices and data from malware and other threats.

8. Be careful when sharing personal information: Be careful when sharing personal information, such as your name, address, and credit card details, online. Only share this information with trusted websites and merchants.

9. Use secure communication channels: Use secure communication channels, such as encrypted email or messaging apps, to protect your sensitive information while communicating with others online.

10. Monitor for potential security threats and breaches and take immediate action if necessary.

Co-funded by the European Union

Overall, the key to effective cybersecurity in international e-commerce is to have a comprehensive security strategy in place that includes a variety of tools and technologies to protect against potential threats.

Thanks!

Co-funded by the European Union