Funded by the European Union

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

HOW TO PROTECT YOURSELF ONLINE?

Practical Recommendations

CYBERSECURITY

– is an essential skill for anyone in the 21st century. With it, you can safeguard yourself from fraudsters and tackle modern challenges. The rules are simple, and they will help you stay safe because cyber threats can be prevented, but dealing with their consequences is nearly impossible.

HOW WILL THE CHECKLIST AND BROCHURE BENEFIT YOU?

The checklist will be useful for your weekly or monthly internet check-up, covering everything from secure access to preserving personal data and using artificial intelligence.

In the brochure, you'll find a detailed description of each checklist item, along with additional recommendations from the author Dana Malikova for more thorough work with programs, your devices, and physical security.

WHO WILL FIND THEM USEFUL?

Everyone! The main condition is that you should be driven by the desire to feel free in cyberspace.

The checklist and brochure will be beneficial for both ordinary individuals and entire organizations, as they are based on the fundamental principles of cybersecurity and include up-to-date recommendations.

INTERNET SECURITY:

1. Public Wi-Fi can become a means of hacking your phone or computer if you connect to it. Moreover, scammers often create a similar network to confuse people, and after connecting to it, you may become a victim of cybercrime.

2. The same can happen if you give the password to your Wi-Fi network to strangers. Being in your network, scammers can hack all devices connected to it.

3. During lockdowns or to access a blocked website, you need to connect to a trusted VPN, as some of them can steal your data. ExpressVPN, Private Internet Access, CyberGhost, NordVPN - the best services of 2024 according to vpnMentor.

4. Phishing is still one of the most effective ways to hack a network, phone, or computer. If you click on unverified links, there is a high chance that scammers can access your devices, steal information, and even apply for credit.

DATA PROTECTION:

1. Some applications ask for more than they provide. For example, a calculator suddenly requests access to your contacts. It's best to deny it, or better yet, delete it right away. Every app you download has a privacy policy - a description of how and why the app will use your data - don't check the box immediately, read them.

2. It's better to pay for an app and be sure it's safe and will update on time. Updates are an important part of all applications' work, like Windows, for example. Often, security solutions and measures against new viruses and cyber-attacks are included in updates to keep you safe.

3. Backing up will help you not lose data if your computer suddenly shuts down or your phone is stolen. You can keep one copy in the cloud, another on a flash drive, and an important document - also print it out in one copy.

4. To avoid being blackmailed by scammers, it's better to keep «sensitive» data «under the pillow», meaning not to share it. Personal photos, ID numbers, addresses, banking details - these are your personal data and they are more valuable than gold.

5. Your password should consist of at least 13 random characters: numbers, lowercase and uppercase letters that mean nothing. Names, nicknames, and birth dates are prohibited. Change them every six months, keep them written down on paper or in a password manager like KeePass.

6. Two-factor authentication is everywhere including Telegram - it's an additional way to log into an app or website. However, it's important not to choose the SMS option, as it's easier to hack; it's better to use push notifications, Google Authenticator, or email.

7. All messengers except Signal are currently very easy to hack, no matter what the manufacturer promises. Therefore, it's unsafe to share important documents in them. Never send ID or other important documents via WhatsApp.

8. Additionally, Signal is the safest app for calls and messaging.

9. It's important to remember that a password is needed not only on your phone but also on your personal and work laptops. If you don't lock your laptop when leaving it in the office or in the room during a coffee break, strangers may have access to all your data.

10. In addition to technical skills, knowledge of Kazakhstani legislation will help you feel more confident and safer online and in everyday life when it comes to protecting personal data and your privacy.

WHAT NEEDS TO BE DONE WITH THE TEAM TO PROTECT YOURSELF AND YOUR PARTICIPANTS?

1. Every organization should prioritize the security of its employees and participants, which is why all processes should start and be based on a privacy policy (otherwise known as a personal data protection policy). Specialists can be involved in its development or it can be developed jointly with the team, using the experience of other organizations.

2. When collecting data from your participants, rely on the privacy policy. During collection, you should explain why you are collecting this data (for example, full name, ID number, address, details, etc.) and obtain consent for the collection, processing, and use, such as publication in a report. Do not collect data that will not be needed for work just «in case». If you don't plan to purchase tickets for participants, you probably won't need their ID numbers.

3. Before taking photos or videos of participants at your events, it's important to notify them and obtain consent for filming and subsequent publication, if you intend to post them somewhere. If someone refuses, you can specify that this person will not be visible during the processing and publication of photos or videos.

4. Basic cybersecurity tools and knowledge are important skills for modern employees. However, threats are constantly «evolving» and changing, so it will be useful for employees to undergo training at least once a year. This way, you will protect your team, as anyone can make a mistake, and the consequences can affect the entire organization.

COPYRIGHT PROTECTION AND NEURAL NETWORKS:

1. Failure to specify the authors of text, video, or photos, besides being an ethical issue, can lead to legal consequences - a pretrial claim. Therefore, ideally, you should first obtain their permission in writing, and then indicate their name.

2. AI can be used to find inspiration and ideas, but not to write important documents; remember that programs already recognize texts generated by neural networks.

3. Deepfakes can be an interesting pastime until they affect the dignity of another person.

4. AI is not the safest means of processing data, so if you use it, be sure to encrypt your data first, at least using digits or alphabetical designations.

This publication was funded by the European Union. Its contents are the sole responsibility of IWPR and do not necessarily reflect the views of the European Union.

kzuncensored.cabar.asia