Дідовець Я., здобувач ступеня вищої освіти
Національної академії внутрішніх справ
Консультант з мови: *Ченківська Н.*

HOW TO PROTECT YOURSELF FROM INTERNET FRAUD

From sophisticated spyware attacks to mass phishing via smartphones and the rise of facial recognition technology, the range and reach of surveillance threats to human rights defenders is growing. Internet crime schemes are different, they steal millions of dollars each year from victims, they steal your personal information and continue to plague the Internet through various methods.

Internet scams come in many forms, including emails that attempt to trick you into handing out financial information, pop-ups loaded with malware, and social media messages crafted to spark fake romantic relationships. The number of complaints of internet crimes jumped 17 percent from 2017 to 2018, according to the FBI's Internet Crime Complaint Center.

Internet scams continue to evolve, and can vary widely. The term generally refers to someone using internet services or software to defraud or take advantage of victims, typically for financial gain. Cybercriminals may contact potential victims through personal or work email accounts, social networking sites, dating apps, or other methods in attempts to obtain financial or other valuable personal information. Many successful internet scams have similar endings: victims either lose their own money or fail to receive funds the fraudster promised. Nowadays smartphones are hacked more often as people use them every day, so smartphones are the main target.

So how to protect yourself from internet frauds? First of all, you can file a complaint with the FBI's Internet Crime Complaint Center, which is the central point for tracking patterns of fraud and abuse related to internet crimes. The center reviews complaints, analyzes data, and creates intelligence reports that highlight emerging threats and new trends. Knowing how internet crimes work helps people understand the dangers involved and identify the fraud before falling prey to it. The center may forward certain investigations to appropriate law enforcement agencies, which may bring legal action against the perpetrators.

After you file the report, the Center recommends keeping any copies of evidence related to your complaint, such as canceled checks, receipts, emails or chat transcriptions. These may help the FBI investigate widespread crimes.

Next methods is setting up multilayered security features. Some online accounts offer an extra layer of security known as multifactor authentication (also called two-factor authentication). This requires two or more credentials when you log in to an account. For instance, this can be a combination of a password plus something you have (such as an additional passcode sent to your phone) or something you are (such as fingerprint or

facial recognition). So if a scammer does get your username and password, multifactor authentication makes it harder to log in to your accounts.

Installing antivirus software is a good idea. Antivirus, or security software is designed to prevent malware from embedding on your computer or device. If the software detects malicious code, like a virus or a worm, it works to disarm or remove it. This could help protect your devices if you accidentally click a dangerous link. The antivirus software can fight the malware and safeguard your files.

When you connect to Wi-Fi in a cafe or airport your internet activities are routed through that network. If attackers are on the network, they could capture your personal data. By using a VPN app on your devices, you protect your online activities when accessing public connections, preventing your internet activities from being seen by others on the same network. If you want to explore options, try NordVPN and TunnelBear.

Always be sure you download software apps and services only from official vendor sites.

Backing up your data is an important thing to do regularly. It's a good idea to regularly make copies of your data in case it's compromised in a malware attack. The backups should be copied to an external hard drive or cloud storage and not your home network. Back up the data on all your devices, including your smartphone.

And the last one, don't trust unsolicited phone calls or emails. If someone calls or emails claiming to be a tech expert, don't accept help, give out personal or financial information, or allow them to remotely access your computer. Instead, ask for proof of identity and research the company.

Therefore, the Internet can be a dark place where virtual thieves can steal your money, your password, and even your identity. But if you follow these rules, you can protect yourself from Internet fraud.

Список використаних джерел

1. URL: https://us.norton.com/internetsecurity-how-to-5-ways-you-can-help-yourself-stay-secure-online.html (дата звернення 06.11.2020).

2. URL: https://www.fbi.gov/investigate/cyber10 critical steps to help protect yourself online (дата звернення 06.11.2020).

Драган Д., курсант Національної академії внутрішніх справ
Консультант з мови: ***Богуцький В.***

COMBATING CORRUPTION IN FOREIGN COUNTRIES

Today, the issue of fighting corruption is most important in every sphere of human life. It threatens the sustainable economic and democratic, social development of the country.

World experience of fighting corruption starts in 1897. There is a large number of world organizations involved in this issue, as well as international legislative acts such as United Nations Declaration against