2. Про затвердження Положення про організацію службової підготовки працівників Національної поліції: Наказ МВС України від 26.01.2016 № 50.
3. Про організацію післядипломної освіти працівників Національної поліції: Наказ МВС України від 24.12.2015 № 1625.
4. Кісіль, З. Р. "Особливості підготовки поліцейських в умовах реформування системи МВС України." Науковий вісник Львівського державного університету внутрішніх справ. серія юридична 4 (2017): 232-238.

Омельчук Д.,здобувач ступеня
вищої освіти бакалавр
Національної академії
внутрішніх справ
Консультант з мови: Гіпська Т.П.

WAYS TO PROTECT AGAINST CYBERCRIME

The recent cyberattack on Transnet's computer systems, which affected the container handling its operations and resulted in ships diverting from South African ports, is still fresh in our memories [1].

Cybercriminals do not only target large multinationals. It does not matter if you are an individual, large, or small company, or even a government entity. As long as you have a virtual identity, your information is a potential target of a cyber attacker.

IT Law defines cybercrime as follows: "Cybercrime refers to criminal activities that specifically target a computer or network for damage or infiltration and refers to the use of computers as tools to conduct criminal activities" [1].

The Cybercrimes Act no 19 of 2020, was promulgated and gazetted on the 1st of June 2021. This Act aims to criminalise offences relating to cybercrime and introduces a framework aimed at the detection, prevention, mitigation, and investigation of cybercrimes [1].

In summary, the Cybercrimes Act refers to cybercrime as:

- the unlawful access to computer systems or computer data storage devices;
- the unlawful interception of and interference with data;
- unlawful acts in respect of software or hardware tools;
- the unlawful acquisition, possession, provision, receipt, or use of a password;
- online fraud, forgery, and extortion.

Our virtual identity is an essential element of our everyday life and criminals use different tactics to obtain personal individual information, information regarding clients, and information regarding suppliers.

Cybercriminals' tactics to obtain information Email and internet fraud Phishing scams Theft and use of your personal information Theft of your card payment information Ransomware attacks.

The impact of a cyber-attack on a company can be detrimental and results in business interruption, reputational damage, and financial loss. The consequences of a cyberattack could also expose the victim to potential claims in terms of the POPI Act, Act no 4 of 2013, effective from 1 July 2021, due to unauthorised disclosure of client personal information [1].

In the Transnet debacle, their computer systems were down for more than a week which resulted not only in huge financial loss to the state-owned entity, but also had a profound impact on the South African economy [1].

Cyber-attacks have increased and are projected to occur every 11 seconds this year.

On an individual level, cybercriminals can obtain access to your personal information and gain access to your financial information and money.

Insurance companies have identified the need and have developed various insurance products to cover individuals and commercial entities against a multitude of risks associated with cybercrime [1].

Stay cyber-safe and remember: “Passwords are like underwear: Don’t let people see it, change it very often and you shouldn’t share it with strangers!” – Chris Pirillo [1].

15 Smart Ways Consumers Can Protect Themselves Against Cybercrime

1. Opt For Automatic Software Updates.

2. Stay Skeptical.

3. Never Reuse Passwords.

4. Use A Password Manager.

5. Leverage Google Authenticator.

6. Always Use A VPN.

7. Confirm All Communications.

8. Adopt A ‘Zero-Trust’ Rule.

9. Stay Away From Links And Attachments.

10. Check Online Breach Reports.

11. Don’t Share Personal Information Online.

12. Never Trust The Default Settings.

13. Don’t Connect To The Internet If You Don’t Have To.

14. Take A Three-Step Approach.

15. Educate Yourself [2].

In conclusion - education is power. Read blogs and/or sign up for online courses around personal security. A good course will cover many critical aspects. Among the words and phrases to search for are “identifying phishing,” “checking SSL certs,” “strong passwords,” “password managers,” “malware scanning,” “system updates,” “malicious files,” “antivirus” and “security settings”.

Список використаних джерел:

1. How to Protect Yourself Against Cybercrime. [Електронний ресурс]. – URL: https://insights.regenesys.net/how-to-protect-yourself-against-cybercrime/

2. 15 Smart Ways Consumers Can Protect Themselves Against Cybercrime [Електронний ресурс]. – URL: https://www.forbes.com/sites/forbestech council/2021/08/26/15-smart-ways-consumers-can-protect-themselves-against-cybercrime/

Пилип'юк В., здобувач ступеня
вищої освіти бакалавр
Національної академії
внутрішніх справ
Консультант з мови: Скриник М.В.

POLICE INTERACTION WITH CITIZENS: INTERNATIONAL EXPERIENCE

The Ministry of Internal Affairs and its system are in the process of reforming and gaining quality international experience. The main thing is to acquire skills with the help of foreign police, namely to transfer skills from other countries.

The result of police activities is interaction with the population and their reproduction.

The police are part of a community that is designed to protect. They are the hope of the people offenders will be punished.

Community Policing is the constant cooperation of the police with the population and local authorities.

The Community Policing approach is based on the principles of constant communication, where:

- the police and the local community are jointly responsible for security;
- the police respond to local needs and demands determined by the community;
- communication between the population and the police is effective and therefore brings results;