УДК 004.5 DOI: 10.33111/mise.97.1

Бабенко Т. В., д-р техн. наук,
професор кафедри кібербезпеки та захисту інформації,
Київський національний університет імені Тараса Шевченка
Галіцина О. В., к.е.н.,
доцент кафедри статистики,
Київський національний економічний університет
імені Вадима Гетьмана

Babenko T. V., Doctor of Science in Engineering,
Professor of the Cybersecurity and Information Security Department,
Taras Shevchenko National Unversity in Kyiv
Galitsina O. V., Candidate of Economic Sciences,
Associate Professor of the Statistic Department,
Kyiv National Economic University named after Vadym Hetman

ОСНОВНІ ПРАВИЛА СУЧАСНОЇ ЦИФРОВОЇ ГІГІЄНИ

BASIC RULES OF MODERN DIGITAL HYGIENE

Анотація. *Цифрова гігієна часто порівнюється з особистою гігієною. Подібно до того, як людина бере участь у певних практиках особистої гігієни, щоб підтримувати власне здоров'я та самопочуття, практики з цифрової гігієни можуть зберігати дані безпечними та захищеними. У свою чергу, це допомагає підтримувати належним чином функціонуючі пристрої, захищаючи їх від зовнішніх атак, таких як зловмисне програмне забезпечення, яке може перешкоджати функціональності. Цифрова гігієна стосується практики та запобіжних заходів, які користувачі вживають з метою збереження конфіденційних даних, організованих, безпечних і захищених від крадіжок й зовнішніх атак.*

Якщо ви запитували когось, чи будуть вони слідкувати за своєю активністю в Інтернеті, ймовірна відповідь ТАК! Насправді багато людей погоджуються з цифровою гігієною і хочуть щось з цим зробити, але просто не встигають або забувають турбуватися. Як і в усіх суспільствах, у кіберпросторі є злодії, шахраї та інші антисоціальні елементи. Відвідувачі повинні застосовувати розумні практики для захисту свого добробуту. Одна велика різниця: ви можете придбати туристичне страхування для більшості напрямків. Немає такої страховки для кіберпростору. Цифрова гігієна — термін, що використовується для опису чистоти чи нечистоти цифрового середовища проживання. Це можна використовувати для опису значків робочого столу, структури файлів, дерев папок, файлів Photoshop або жорсткого диска, сторінки Facebook або цифрових персонажів. Так само, як організм може стати нездоровим через накопичення поганих харчових продуктів, жорсткий диск людини може стати нездоровим завдяки накопиченню вірусів, піктограм і фрагментарного програмного забезпечення. Гігієна відноситься до практики, пов'язаної із забезпеченням міцного здоров'я та чистоти. Науковий термін «гігієна» означає зміст здорового та здорового життя. Термін з'являється у таких фразах, як особиста гігієна, побутова гігієна, гігієна зубів і гігієна праці, і часто використовується у зв'язку із здоров'ям населення.

Ключові слова: *цифрова гігієна, кіберпростір, інформаційні технології, конфіденційність, інформаційне суспільство.*

Abstract. *Cyber hygiene is often compared to personal hygiene. Much like an individual engages in certain personal hygiene practices to maintain good health and well-being, cyber hygiene practices can keep data safe and well-protected. In turn, this aids in maintaining properly functioning devices by protecting them from outside attacks, such as malware, which can hinder functionality. Cyber hygiene relates to the practices and precautions users take with the aim of keeping sensitive data organized, safe, and secure from theft and outside attacks.*

Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

If you asked someone whether they would look after their online presence, the likely response is YES!, however in reality, it's unlikely that they would do simply because it's another thing to add to the daily hustle and bustle of life where we are already stretched as it is — we've talked about our findings from the last 12 months on another post so we won't go Into detail, but essentially we confirmed that lots of people agree with digital hygiene and want to do something about it, but simply don't have time or can't be bothered.

Like all societies, cyberspace has thieves, fraudsters and other antisocial elements. Visitors should adopt sensible practices to protect their well-being. One big difference: you can buy travel insurance for most destinations. there is no such insurance for cyberspace. Digital hygiene is a term used to describe the cleanliness or uncleanliness of one's digital habitat. This can be used to describe one's desktop icons, file structure, folder trees, Photoshop files or harddrive, Facebook page or digital persona. Just as one's body can become unhealthy by the buildup of poor food choices, one's hard drive can become unhealthy by the buildup of viruses, icons and fragmented software. Hygiene refers to practices associated with ensuring good health and cleanliness. The scientific term «hygiene» refers to the maintenance of health and healthy living. The term appears in phrases such as personal hygiene, domestic hygiene, dental hygiene, and occupational hygiene and is frequently used in connection with public health.

Keywords: *digital hygiene, cyberspace, information technology, privacy, information society.*

Вступ: There was a time when we were read stories before going to sleep some of these stories involved beautiful princesses and knights in shining armor. Others were scary with Big Bad Wolves, Witches, curses, poisons and other nasty elements. Yet, many of the stories had a purpose beyond getting a child to sleep, and one old favorite, the story of the Three Little Pigs and the Big Bad Wolf, is relevant our thesis.

No doubt you recall that the Big Bad Wolf (BBW) wanted to eat the little pigs (LP). Two of them wanted to play and dance and built their houses quickly — one with straw and the other with branches. Of course the BBW blew them away with little effort.

It was only the third and most serious LP who decided to build a house carefully, using bricks and mortar so that it could not be easily blown away. And so, transferring this story to cyberspace, where there are no BBWs, there are many other characters with malicious intent.

Statement of problem: Most of us think of «hostile» parties as having strong bodies, being armed, faces hidden by masks or helmets and exhibiting menacing behavior.

The reality is that malicious actions in cyberspace involve well educated, smart, creative individuals with a good knowledge of information technology.

Main vesults: The list of the inhabitants of cyberspace's hostile side is not comprehensive and evolves through human creativity. Gaps in legislation, that develops at a slower rate than new forms of crime, allows hostile elements to act with impunity and immunity [1].

- In fact, you yourself could be the problem when your electronic devices have been compromised and are used to spread malware, spam or messages pretending to be from you but sent by a third party with malicious intent. USB flash memories (also called thumb drives) are notorious offenders.
- Someone, deliberately. It does happen, in the form of fraud, sabotage, theft of intellectual property, planting compromising information on someone else's devices, etc.
- Individual hackers. They could be anyone, anywhere, with good technical skills who choose to target a specific individual or organization. In 2002, a young Scotsman successfully committed what was described at the time as «the biggest military hack of all times» involving 97 US military and NASA computers. A request to extradite the individual to the USA, where the military hack took place, was denied by his country of origin on humanitarian grounds.
- Malware suppliers. The design and distribution of malware has become a business (An article in the Economist referred to this as Crimeware As A Service or CaaS). Custom made malware designed to target a very specific target has been, designed, the best known being the Stuxnet malware used in 2010 to sabotage uranium enrichment facilities in Iran.
- Professional hackers. The equivalent of a gun for hire, those who operate unethically specialize in the field of private detectives, industrial espionage and theft of intellectual property.
- Happily, many such professionals provide a service that tests the effectiveness of protective measures implemented by organizations. Called Ethical Hacking or Penetration Testing, it provides a «second opinion» (for a fee).

- Hackers with the a cause. These are legally punishable offences but require the perpetrator to be caught and that the digital forensic evidence complies with legal requirements). It may also involve a non-criminal offence like giving you an infected USB memory as a gift that may not contain malware but has instead copies of copyrighted material.
- Cyber criminals. Working alone, in small groups or as part of Organized Crime, their motivation is primarily financial. They are behind the most successful scams that get individuals to give them money because they believe their stories.
- Non-state actors. Usually referred to as «terrorists» or equivalent terms, their motivation is the disruption of civil society and governments.
- State sponsored. Referred to as «cyber-armies», these are increasingly being mentioned in the Media but rarely, if ever acknowledged by governments. Clearly, the gathering of Intelligence and Counter-intelligence the context of National Security is neither new nor unusual — the tools have changed. There is considerable debate about what might be the appropriate balance between defensive measures and offensive capabilities.

Happily feeling secure and private behind our screens — regardless of the device used, it is easy to forget that every action in cyberspace is recorded somewhere by someone for various reasons, all of which imply knowing more about you and what you do in cyberspace. Recent media reports have confirmed what information professionals have known for years: monitoring it is possible and we have the technology to do it. Every technology has the potential to be misused and abused [2].

For the sake of an example, on August 4, 2013, there were media reports about a family from New York State, USA, who were detained and interrogated under suspicion of terrorist activity. The story revolves around «Mother» searching for pressure cookers, «Father» searching for backpacks and «Junior» wanting more information on the Boston Marathon bombings of 2013 [3]. The monitoring computers correlated these searches and reported a potential terrorist threat.

Given the massive flows of data across the Internet and the global telephone networks it would be impossible for «people» to watch all of it. But what is too much for humans is digestible for computers which can therefore monitor all or parts of all this traffic and be programmed to produce appropriate reports.

Some of the parties that know what you are up to with your devices are the obvious ones like your Internet Service Provider and your mobile communications provider. But there are many others. If you are using your employer's networks and/or devices your activities may be tracked by your employer. Legislation about this varies from country to country.

It really depends on how each individual feels about «privacy» and the extent to which each society applies the concept of «freedom of speech». While the latter is the subject of Article 19 of the United Nations Declaration of Human Rights of 1948, the Article recognizes that such freedom has limitations.

The most common limitations include items such as: slander, libel and defamation, the disclosure of confidential information, obscenity, etc. The World Summit on the Information Society of 2003 made a statement on the importance of the freedom of expression for the Information Society [4].

The Internet and other innovations in Information Technology have fundamentally changed the way in which we interact with organizations, with each other and, in turn, these changes have had a major impact on how we understand «privacy».

The figure illustrates the many information exchanges that begin with us as individuals. This first section on disclosures examines those we do because we are required by law and/or contract.

Disclosures required by law tend to be government requirements. Dese include civil status (births, marriages, divorces, deaths), property records, taxes, social security, driving licenses, etc. [5].

Historically done on paper, the adoption of e-government around the world is moving us into an environment where information about individuals is in electronic form and therefore easier to search (no need to dig into a dusty archive in a dark basement).

Disclosures required by contract include those related to employment, where an individual needs to provide details such as address and contact numbers, dependents, bank accounts, diplomas and certificates, etc. They are also required by banks, insurance companies, airlines and other businesses.

The Internet Of Things (IOT) will take this much further by giving objects an identity that can be accessed and verified electronically. The figure below gives a summary of the current status of the IOT and how it may develop.

There is much optimism about the many benefits that an IOT will bring and enthusiasts talk of up to 50 billion devices being connected to it [6]. Driven by Venture capital, commercially motivated vendors, designed by geeks and rushed to the market, we can expect many unintended consequences.

The 2003 World Summit on the Information Society took place in 2003 [7]. The Diplo Foundation (www.diplomacy.edu) produced and published a series of booklets under the umbrella title of «Information Society Library» — several of these booklets focused on information security and one of them addressed Good Hygiene. The mindmap below summarizes the topics covered.

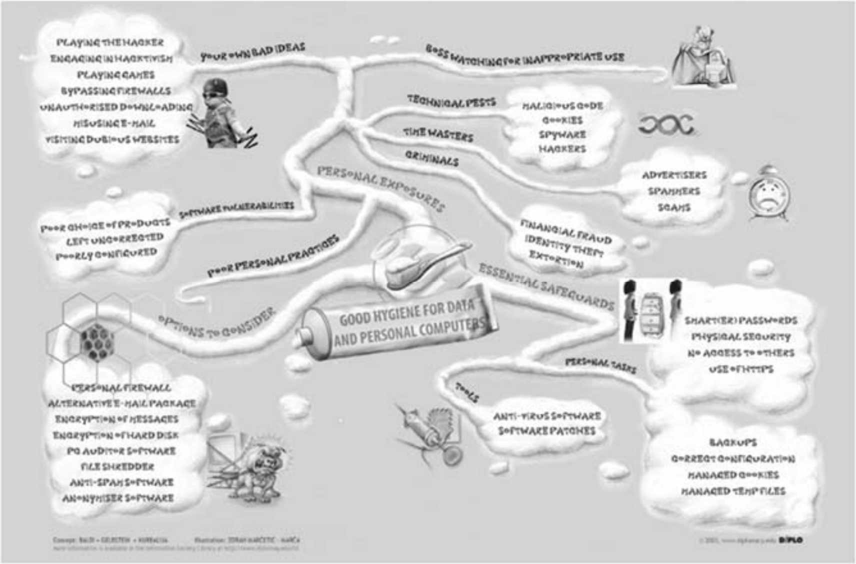

Fig. 1. Map of good hygiene for data and personal computers

Looking back ten years is instructive as it highlights the explosive rate of growth of the interactive electronic world and how much the need for good hygiene has changed.

The term «Web 2.0» was first used in 1999 and marked a departure from the static catalog style of web pages and the emergence of «anyone can be a content creator» that characterizes the web in 2013 [8].

The «smartphone» — a device that combines telephony with computing capabilities was first commercialized in the mid 1990s and these found a measure of adoption in the corporate world. The introduction of the iPhone in 2007 created a popular market for these devices and its thousands of applications (apps) [9]. The emergence of tablets and other models of smartphones just increased the need for end users to protect themselves from the dark forces that inhabit cyberspace and the need to practice good hygiene will grow and continue to evolve.

The Internet Of Things (IOT) will take this much further by giving objects an identity that can be accessed and verified electronically [10]. The figure below gives a summary of the current status of the IOT and how it may develop.

Summary: signs of slowing down and attempting to predict which developments will be successful is a matter for gamblers willing to invest in promising consumer oriented initiatives and see what happens.

Where such innovations will take society is another unpredictable topic. What we should have learned by now is that the ease of use of such products hides a great deal of complexity, and this, in turn, the reality that all such products contain imperfections — the author refers to them as «bugs» while some of the designers call them «features».

This is understandable when we consider the many parties involved in delivering innovative technologies. Looking at smartphones for example, they require the fusion of the work of:

All of the persons who engaged in creating the item work independently of each other and deal with devices of such complexity that no amount of testing prior to production can identify 100 % of the possible vulnerabilities and bugs. This complexity is hidden from the end user. When this person is unaware of how to protect the device and the data it contains, disappointment, frustration and headaches are likely outcomes.

The main lesson that can be drawn from it is that the creative ideas of the world of fiction can successfully migrate to the real world — it may take many years and many failures. The impact of successful initiatives on society and individuals can introduce significant change as well as undesirable and unpredictable side effects.

References

1. Protecting Yourself Online — What Everyone Needs to Know n. d., Australian Government <http://www.staysmartonline.gov.au/data/assets/pdf file/0005/19598/Protect yourself online.pdf>

2. Cyber OPSEC USA Interagency Support Staff n.d., <http://www.dodea.edu/Offices/Safety/upload/15 Cyber Protecting Yourself Online.pdf>

3. Staying safe on the Internet, Interpol n.d., <www.interpol.int/content/download/. ../Education-SafelnternetEN.pdf>

4. Mobile security survival guide for journalists n.d., <https://www.aswat.com/files/Mobile %20Iournalist %20Survival %20Guide.pdf>

5. Protect Your Computer From Viruses, Hackers, and Spies n. d., State of California, http://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer

6. Online Safety How to Protect Yourself and Your Family, Ministry of Education, Trinidad and Tobago n.d., <http://www.moe.gov.tt/laptop info/Online Safety Tips.pdf>

7. The World Summit on the Information Society, Geneva , accessed 12.12.2003, < https://www.itu.int/net/wsis/>

8. USA Government n.d., <http://www.usa.gov/topics/family/privacy-protection/online.shtml>

9. Good practices n.d., The National Cybersecurity Agency of France, <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/ >

10.Be secure online n.d., UK Government services http://www.nidirect.gov.uk/be-secure-online

Additional

1. Protecting Yourself Online — What Everyone Needs to Know n. d., Australian Government <http://www.staysmartonline.gov.au/ data/assets/ pdf file/0005/19598/Protect yourself online.pdf>

2. Cyber OPSEC USA Interagency Support Staff n.d., <http://www.dodea.edu/Offices/Safety/upload/15 Cyber Protecting Yourself Online.pdf>

3. Staying safe on the Internet, Interpol n.d., <www.interpol.int/content/download/. ../Education-SafeInternetEN.pdf>

4. Mobile security survival guide for journalists n.d., <https://www.aswat.com/files/Mobile %20Iournalist %20Survival %20Guide.pdf>

5. Protect Your Computer From Viruses, Hackers, and Spies n. d., State of California, http://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer

6. Online Safety How to Protect Yourself and Your Family, Ministry of Education, Trinidad and Tobago n.d., <http://www.moe.gov.tt/laptop info/Online Safety Tips.pdf>

7. The World Summit on the Information Society, Geneva , accessed 12.12.2003, < https://www.itu.int/net/wsis/>

8. USA Government n.d., <http://www.usa.gov/topics/family/privacy-protection/online.shtml>

9. Good practices n.d., The National Cybersecurity Agency of France, <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/ >

10.Be secure online n.d., UK Government services <http://www.nidirect.gov.uk/be-secure-online>

Статтю подано до редакції 01.03.2019 р.