

УДК 681.51

Andrey Budyonnyi¹, Yuliya Sobol²

¹ student of group RT-810, National University «Zaporizhzhia Polytechnic»

² PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

DIGITAL INFORMATION SECURITY

We live in a time when most of our lives, personal and professional, resides online. We do our banking, music purchases, bill paying, social planning, and even

parts of our job, in the digital world. This increased reliance on the internet and digital networks brings risks along with the convenience it provides.

Online criminals, hackers, even just bored mischief-makers lurk in the shadows, waiting to rob you, commit fraud, steal your identity, or simply embarrass you. Therefore, digital information security is of paramount concern.

Digital security is the collective term that describes the sources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices. In other words, digital security is the process used to protect your online identity.

Cybercriminals are opportunists attracted by the sheer volume, value, and variety of data available for exploitation. And all they need is just one good haul to make their efforts worth it. If they can fool only one consumer—through a phishing attack, for example—hackers could reap the rewards of a stolen identity or a compromised credit card with a substantial balance to burn through.

Like we said at the start, our increased reliance on the internet means we have a lot more to lose if something goes sideways. The stakes are high; we need impeccable, reliable digital data security.

Not every bit (or byte) of your information is useful to cybercriminals. A total stranger finding out that you prefer the original Star Wars trilogy to the sequels is scarcely an earth-shattering revelation that could compromise your identity or financial security. So, what kinds of data are at risk?

Personal Identification Data. This data includes your name, phone number, address, email account name, IP address, and, most damaging, your Social Security number. It also includes information that potentially pinpoints your location. Personal data is often used for identity theft and social engineering. Also, a hacker who has your Social Security number (or equivalent) can open credit card accounts in your name, thereby eventually destroying your credit score.

Personal Payment Data. If it has to do with financial transactions, it's considered personal payment data. This information includes credit and debit card numbers (including expiration dates), online banking numbers (account and routing), and PIN codes. Criminals who gain access to your online banking information can even transfer funds out of the accounts or make purchases.

Personal Health Data, also known as personal health information (PHI), encompasses information on your health, including medical history, prescription drugs, health insurance subscriptions, and doctor and hospital visits. This information is precious to high-rolling cybercriminals since they can use your health information to file false insurance claims or order and resell prescription drugs.

As we can see, hacks can occur in many information pathways on the Internet. Business organizations, mainly small and medium-size, face critical challenges in protecting data. Limited financial and technological resources make it difficult for them to upgrade security systems and to stay updated with technology. However,

better awareness towards cyber security and proper planning can prove to be very beneficial for such business organizations in protecting their information and trade secrets from being disclosed. Many small business organizations are now taking initiatives to protect their information from being accessed illegally.

Cyber security is equally important for local, state, and central government as these organizations maintain a huge amount of confidential data and records concerning the country and its citizens. Yet several government organizations face difficulty in protecting data because of inadequate secured infrastructure, limited funding and lack of security awareness. Stealing of confidential data or sensitive information, digital by terrorists from government organizations, as well as digital spying can lead to serious threats to the country. For this reason, cyber security is of paramount importance for government organizations also and is a vital asset to the nation.

The increasing use of the internet and social media has made cyber security even more important than it was before. Growing cyber threats such as data theft, phishing scams and other cyber vulnerabilities demand that users should remain vigilant about protecting data. It is essential to understand the varied type of risks and vulnerabilities that exist in the Internet world. For every user it is important to think before connecting to someone using online medium. Users should also think prior to sharing any information with other users through the internet.