M. Bahrii, Student
N. Shkoliar, PhD in Ped., As. Prof.
Khmelnytsky National University

CYBER HYGIENE: ESSENTIAL FOR DIGITAL SECURITY

In the current digital world, it is crucial to prioritize cybersecurity measures in order to protect confidential data from cyber attacks. One of the most important aspects of cybersecurity is cyber hygiene practices, which involve taking a number of precautions to protect personal data and ensure the functionality of devices and systems. By regularly following cyber hygiene rules, individuals and organizations can prevent cyber attacks and protect themselves from theft or damage to confidential information. Cyber hygiene is essential to maintaining the integrity and security of personal data, which if not followed, can lead to cybersecurity breaches. Therefore, it is vital to understand the importance of cyber hygiene and take regular measures to protect against cyber threats.

The cybersecurity industry faces a number of constantly evolving threats, including malware, phishing, and the use of emerging technologies such as machine learning and crypto currency. The lack of qualified cybersecurity professionals exacerbates these risks, which can lead to leakage, distortion, and degradation of information. This is already slowly leading to the growing likelihood of Internet outages, disinformation, and conflicting privacy rules now. In addition to the above threats, the cybersecurity industry is also facing challenges from the growth of Internet of Things (IoT) devices, cloud computing, and the increasing use of artificial intelligence (AI) and automation technologies. As the number of devices connected to the Internet increases, the attack surface for cybercriminals expands, creating more opportunities for them to exploit vulnerabilities. Cloud computing has also created new risks as many organizations rely on third-party providers to manage their data and applications. While cloud providers offer robust security measures, misconfigurations and other human errors can still lead to data breaches. The use of artificial intelligence and automation technologies also creates both opportunities and risks. While these technologies can help identify and respond to threats faster and more efficiently, they can also be used by cybercriminals to develop more sophisticated attacks. Overall, the cybersecurity industry is facing an ever-changing threat landscape, with new risks and challenges emerging every day. To meet these challenges, organizations and users must also prioritize good cyber hygiene practices, such as regularly updating software and implementing strong passwords, to protect against common threats and reduce the risk of successful cyber attacks. Creating and enforcing a cyber hygiene policy is crucial for maintaining the security of your network and information. This policy should include regular maintenance practices and continuous user education. Using the right cybersecurity tools, such as antivirus software, network firewalls, and password protection, can also help protect your network. Implementing secure authentication and access policies, such as using strong passwords and multifactor authentication, is important for limiting access to authorized users. Confirming endpoint protections and employing a cybersecurity framework can further strengthen security measures.

Finally, backing up data to a secondary location is essential for ensuring that the data is not lost in the event of a breach.

To ensure good cyber hygiene the following measures should be taken:

Keep passwords safe and secure: avoid using the same password for different accounts, change passwords regularly, use strong passwords, change default passwords on IoT devices, avoid writing down or sharing passwords, and use a password manager. Use multi-factor authentication: protect essential accounts with MFA and save backup codes in the password manager. Back up data regularly: keep files secure and protect against data loss by backing up essential files offline. Ensure privacy: don't post private information publicly on social media, review social media privacy settings, avoid quizzes/games/surveys asking for sensitive information, be cautious about app permissions, lock devices with a password/PIN, be careful on public Wi-Fi, use a VPN, make online transactions via secure websites, and share information about online privacy with family and friends. Keep apps, software, and firmware up to date: update regularly, set up automatic updates, delete unused apps, and download only from reputable/official sources. Secure routers: change default name/username/password, keep firmware up to date, disable remote access/UPnP/WPS, set up a separate network for guests, and use WPA2/WPA3 encryption. Avoid social engineering attacks: do not click on suspicious links/emails/ads.

Use network firewalls: use a firewall to prevent malicious software from accessing the computer or network via the internet, and ensure it is correctly configured. Encrypt devices: encrypt devices and other media containing sensitive data. Wipe hard drives: wipe hard drives clean before disposing of or selling a device. Ensure high-quality antivirus protection: use high-quality antivirus software and keep it up to date.

One of the most talked-about security events of the 2020 was at the Oxford University, Division of Structural Biology lab that conducted research on the COVID-19 vaccine. In this incident, threat actors were able to compromise internal lab systems and gain unlimited access to coronavirus research data, biochemical sample data, and more. Although the university failed to disclose the scope of the data breach, it is clear that the damage is already done. In this scenario, the fallout from this cyber-attack could be the loss of intellectual property. It could have been avoided by means of zero-trust and device authentication: Oxford University could have stayed out of the headlines if they took a zero-trust approach and prevented unauthorized users and devices from accessing internal systems.

In conclusion, good cyber hygiene is essential for protecting your personal and sensitive data online. By following these best practices, including using strong passwords, keeping your software up to date, and using two-factor authentication, you can significantly reduce the risk of cyber attacks. Remember to regularly backup your data, limit your exposure to public Wi-Fi, and practice safe online shopping. Educate yourself on cybersecurity best practices and monitor your accounts for suspicious activity to ensure that your digital life remains secure.

REFERENCES

1. https://nordvpn.com/uk/blog/cyber-hygiene/

2. https://intone.com/importance-of-cybersecurity-in-the-current-digital-world/ https://securityscorecard.com/blog/what-is-cyber-hygiene/

https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

3.https://artmotion.eu/en/insights/blog/top-3-data-breaches-and-how-they-could-have-been-avoided.html