SECURITAS

Intelligence Bulletin 12/02/19

Securitas Intelligence Unit

Managing Cyber Threats: Personal Cybersecurity Tips

The total cost of cybercrime committed across the world last year exceeded $1 trillion dollars.[1] Although famous cases have targeted corporations, banks and government infrastructure, attacks on individual users have greatly contributed to the total losses. Over 95% of cybersecurity breaches are through human error.[2] Cyber-criminals and hackers infiltrate the sensitive information of both companies and individual users through the weakest link – human fault. Hackers have the capacity to hijack usernames and passwords, make purchases, request new PIN numbers, open credit cards under stolen identities and sell information to third parties who can use it for illicit purposes. Advice for businesses can be found in the previous instalment of this cyber series. Personal vigilance measures can help mitigate threats to individual users:

Download the Latest Software Updates

Ransomware attacks can escalate through outdated software in both operating systems and applications. Installing the latest software updates can remove critical vulnerabilities that hackers exploit to access devices. Keeping browser plugins such as Flash, Java, etc. updated and turning on automatic system updates for your devices helps to keep on top of the latest patches.

Passwords and Multi-Factor Authentication

Strong passwords are critical to online security, with weak passwords being an easily exploited tool for hackers. Users are advised to avoid using the same password twice, never to leave a password hint where a hacker could access it, and to use at least eight characters when formulating passwords. A password management tool is a useful method of keeping passwords safe and secure. Two-factor and multi-factor authentication provides multi-layer security that can deter cyber-threat actors. With additional authentication, users may be asked to enter a further pass code, additional password or even a fingerprint.

Phishing Scam Awareness

In a phishing attempt, the attacker poses as a benign actor to trick the recipient into divulging personal information, clicking a malicious link, or opening an attachment that installs malware or a trojan horse onto the user's system. This is by far the most common cause of ransomware attacks, with 90% of malware attacks stemming from phishing attempts.[3] Do not open emails from people you do not know. A common tactic used by cybercriminals is to forward the virus from the victim's device to their contacts, so always remain sceptical of any links. Grammatical errors and unofficial web addresses are usually a giveaway for scams; hover over any links to inspect where they direct to.

Regularly Back Up Data

Backing up data will restore any files lost to ransomware or malware. A simple strategy endorsed by cyber experts is the '3-2-1 rule'.[4] In essence, this means storing three copies of your data: one copy on a local drive, one on an external hard drive, and one copy in an offsite location, potentially cloud storage.

Avoid Public Wi-Fi and Insecure Networks

It is recommended not to use public Wi-Fi without the use of a Virtual Private Network (VPN). Using a VPN ensures encryption, meaning it adds further complexities for cybercriminals attempting to access data on your device.

[1] https://www.cybintsolutions.com/cyber-security-facts-stats/

[2] https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

[3] http://blog.cipher.com/10-personal-cyber-security-tips-cyberaware

[4] http://blog.cipher.com/10-personal-cyber-security-tips-cyberaware

If you would like any further information on any of the elements mentioned in this bulletin, please email the Securitas Intelligence Unit at:

soc.intelligence@securitas.uk.com

February 2019