PAUL KANG - *Co-Founder / Director, ENTERSOFT*
https://www.linkedin.com/in/pkangduck/

Paul is a co-founder and Director of Entersoft, a global award-winning Cyber Security Company helping organisations secure their digital assets. He has been identifying, evaluating and developing business opportunities for Entersoft to expand into new territories whilst establishing relationships/partnerships with stakeholders across the Asia Pacific.

TIP 1. PRIORITISE EMPLOYEE CYBER AWARENESS

Staying vigilant when it comes to cyber security is essential for the health and sustainability of any small business. Basic cyber security practices and policies must be adhered to by all employees. This begins with proper training around the importance of strong passwords, the handling of customer data and awareness of phishing scams and suspicious downloads.

TIP 2. STAY UP TO DATE WITH SOFTWARE UPDATES TO PROTECT INFORMATION

Always ensure that the latest software is installed on all of your operating systems. To combat the rapidly evolving hacker playbook, companies must stay on top of any software improvements to fix existing loopholes. Updated software, web browsers and operating systems provide your business with the best chance of preventing an attack. It's also important to run antivirus software for scanning purposes after each update.

TIP 3. LIMIT THE ACCESS TO DATA

Cyber security vulnerabilities can be exploited both externally and internally. These internal threats are often employees within the organisation who may indulge in malicious practices. The most effective method of defence against such threats is to limit individual employee access to data and sensitive information. Employees should also be required to request permission prior to installing any software.

TIP 4. PASSWORD SECURITY AND TWO-FACTOR AUTHENTICATION

Create unique and strong passwords for employees which can be a combination of numbers and letters with special characters. Avoid using personal information like birth dates and phone numbers as passwords. Always activate two-factor authentication and limit the number of password attempts at all stages of the authentication process.

TIP 5. SECURING MOBILE DEVICES

Mobile devices are extremely vulnerable to cyber-attacks. Unprotected mobile devices present significant security risks if they hold confidential information, or have access to corporate websites when used on public networks. It's imperative that employees protect all data via passwords, encryption and security apps. They must also immediately report any devices that have been lost or stolen.

TIP 6. ALWAYS STORE BACKUP COPIES

It should be common practice for organisations to keep a backup of all important information and sensitive data relating to both the business itself and its clients. These can include spreadsheets, word documents, financial and human resources files and customer data. It's also recommended that you store all confidential data across multiple backup locations, i.e. on cloud, on-premises, this will allow for the immediate reinitiating of all relevant data in the event of an attack.

TIP 7. SECURE PAYMENT SYSTEMS

While processing payments, crucial and sensitive customer information is exchanged. In order to protect the aforementioned data, we recommend using separate computers for processing payments and surfing the internet.

TIP 8. BE AWARE OF THE DATA YOU COLLECT

Businesses collect a variety of data from customers such as names, numbers, dates of birth, addresses, emails, account details etc. It's crucial that businesses streamline this process and only ask for essential data plots. By reducing stored confidential data, businesses can effectively reduce their risk.

TIP 9. MIGRATE TO THE CLOUD

Robust Cloud security is one of the most effective methods of preventing cyber attacks. For most small businesses, storing confidential data on the Cloud is far more secure than on a local server. In most Cloud security exploits, attackers take advantage of misconfigurations in the Cloud. We recommend getting in touch with a reputable cloud security provider while utilising any built-in Cloud protection services.

TIP 10. GO WITH THE EXPERTS

Cyber security is the most essential part of any modern business. Small businesses are often unable to cope with the ever-present threat of cyber attacks and, as a result, they can face devastating losses. By enlisting the services of cyber security experts, you're providing your business, and your clients, with peace of mind, while freeing up crucial time and capital that can be deployed elsewhere. We also recommend taking out cyber security insurance for added protection.