InternetNow Security Health Check-up for SME

October 2017: SME in Petaling Jaya lost a payment amounting to USD200,000 (roughly RM844,700) from a Europe-based customer because their business email was compromised.

August 2017: A local bookstore chain was infected by Ransomware. Huge amount of valuable data was lost.

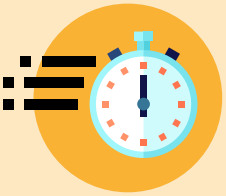
July 2017: A 200-employee public-listed company in Kuala Lumpur encountered CEO-fraud incident, instructing for an urgent payment of RM70,000 to be made to a local bank account.

The cyber threats facing Malaysian Small & Medium-sized Enterprises (SME) are real which are costing the SMEs millions of Ringgit in damages in terms of direct losses, operational downtime, and reputational damages.

However, many business owners are struggling to secure their IT infrastructure due to a few reasons:

Lack of expertise: SME's IT personnel are usually not security specialists

A medical field analogy might be applicable. Many of the IT staff employed by SMEs are similar to General Practitioners (GPs). They are expected to know a bit of everything so that they can support various aspects of the company's IT needs. But to address security risks, what is needed are Specialist Doctors.



Fast-changing security landscape: New threats and vulnerabilities are discovered every week making it difficult to keep up.

Poorly managed security products: Companies are investing in security products, however are they configured correctly, and maintained properly (in terms of monitoring or being updated to the latest version).

Why Security Health Check-up

Many IT security consultants recommend products as a mean to solving security problems while still lacking basic security hygiene whereby the basic security best practices are not followed (such as enforcing strong passwords and etc).

What is InternetNow Security Health Check-up For SME (ISHC)

ISHC helps to plug the common security gaps in an SME.

Firstly, our focus is on the email system because this is the main target of the cyber criminals while checking if someone is already intercepting your mails.

Secondly, we will check if there's any confidential files that are shared openly to the rest of the company.

Scope of checkup

Area	Description
Section: Email	
Password strength	Ensure email passwords are at least 8 characters and strong (eg: internetNOW@1234). No sharing of passwords is permitted.
Email forwarding	We check if all email forwarding enabled are intended while providing the list of email addresses to enable verification.
External email access restriction	Most companies give external email access to all staff however some office-bound staff do not need this feature. Therefore we can reduce the risk of their emails being hacked by disabling external email access for them.
Safer, higher email ports	We check the ports of your mail server. If the ports are using the standard port numbers, then we will reconfigure them to higher port numbers.
Brute-force Protection	We check existing mail server has brute-force protection for common protocols (SMTP, POP3, IMAP).
SSL Implementation	We check if SSL is currently enabled for the common protocols.
Sender Policy Framework (SPF) Implementation for own domain	We check if your own domain is SPF configured.
Section: Data Privacy	
Open Folder sharing	We will scan for any confidential folders that is openly shared to everyone in the network.

InternetNow! The Internet Specialists
www.internetnow.com.my

INTERNETNOW TEKNOLOGI SDN. BHD. (721490-V)
Tel. : 603-8075 2050 Fax : 603-8075 2686 Email : enquiry@internetnow.com.my
2F-18 & 19, IOI Business Park, Persiaran, Puchong Jaya Selatan, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan.