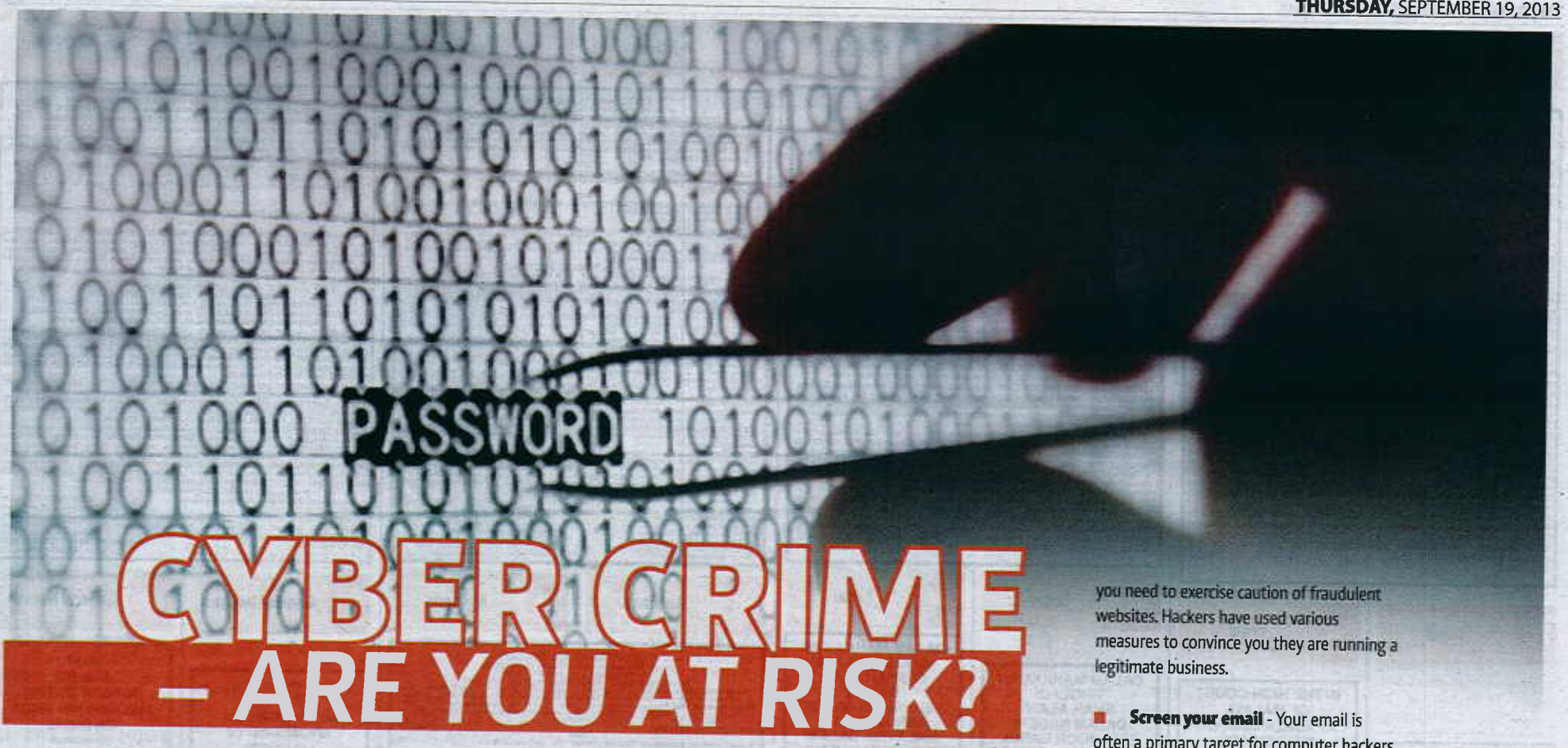

CYBER CRIME – ARE YOU AT RISK?

WE are currently living in the Cyber Age, where Internet and computers have major impacts on our way of living, social life, and the way we conduct businesses.

However, with the growth of the internet, network security has become a major concern as cyber crimes have emerged rapidly in the last few years.

Cyber crime may include activities such as computer hacking, spam marketing, credit card fraud, identity theft, email scam, and many more.

The more traditional form of attacks is releasing of malware, spyware, and viruses to disrupt computer operation and gather sensitive information.

To protect yourself from being the victim of the machinations of cyber criminals, you need to take some proactive measures.

- **Protect your PC with comprehensive security software** – Anti-virus software alone is not enough to provide full protection for your PC. You also need comprehensive protection from malware, phishing, spyware, and other common and emerging threats. Just make sure that you keep your security software up to date and don't forget to perform regular scans.

- **Set up a strong password** - A strong password should have at least 10 characters and consists of a combination of letters, numbers, and special characters. It is recommended that you change your password periodically to reduce the chance of it being compromised. Avoid obvious passwords such as your name, your nick name, and date-of-birth etc.

- **Enable firewall protection** - Firewall protects a computer network from unauthorised access. Network firewalls may be hardware devices, software programmes, or the combination of the two. A network firewall typically guards an internal computer network against malicious access from outside.

- **Secure your wireless network** - Most routers and access points have an administrator password that is needed to log into the device, and modify any configuration settings. As soon as you set up a new WLAN router or access point, your first step should be to change the default password and enable the routers firewall. Check the owner's manual for instructions.

- **Protect your personal information** - Some websites require you to enter your personal information while filling out an online application form. Since you cannot prevent divulging your personal information, you need to exercise caution of fraudulent websites. Hackers have used various measures to convince you they are running a legitimate business.

- **Screen your email** - Your email is often a primary target for computer hackers looking to steal personal information, financial data, security codes, and even download viruses and malware into your computer. Do not simply open any links in emails from people you are not familiar with. Even if the message is from someone you know, be cautious. Look for information to verify the mail is genuine.

- **Go e-shopping on trusted and secure websites only** - The website is secure if it has a URL starting with "https" instead of the usual "http". Websites that bear a VeriSign or TRUSTe seal is also more secure. If the website does not have these, then you are potentially uploading your credit card and other private details to a possibly fraudulent site.

- **Be wary of phishing sites** – Do not to log on to any financial sites by using a link that was emailed to you. The link can take you to a site that can grab all the details you enter, such as your username and password. The hacker can make use of this information to make transactions. If you need to access these sites, go to the official site by typing the address into your menu bar.

- **Monitor your children's online activities** - They may not know it, but some websites may contain threats to your computer. You can install parental control applications or software to restrict the type of sites your child can view.

- **Scan any email attachments** - Beware of files downloaded from the Internet before opening them. This is to ensure there is no malicious programme in the download. Never download an email attachment that is not from a trusted source, especially if it has the .exe extension. Scan any flash disks, or other storage media before use.

- Compiled by **1Klassifieds** *Team*