MACROKIOSK

STAY SAFE from Digital Deception

As the world comes to a near standstill, digitisation is essential in helping businesses to keep going and many have fast-tracked their digital transformation to cater to the surging demands.

As such, threats to cybersecurity is prevalent, especially now more than ever, and it is highly crucial for businesses to safeguard their digital assets, whether it is their payments platform, communication channels or infrastructure.

MACROKIOSK, an ISO27001 ISMS certified company, adheres to strict policies and stringent practices to ensure uncompromised security and safety of our solutions, handling of data and operational procedures which serve more than 3000 clients in 37 countries spanning 24 industries.

As much as we can do on our part to provide clients with a safe and secure environment while using our solutions in their business dealings, we strongly recommend clients to conduct due diligence in mitigating cyber-attacks and threats.

Here are some recommendations from Mr. Patrick Hew, Chief Technology Officer of MACROKIOSK, to help you enhance your cybersecurity practices:

REINFORCE ICT INFRASTRUCTURE

Schedule regular maintenance of Information and Communication Technologies (ICT) infrastructure and assets to ensure your systems are working at optimal conditions to support your business and customers. Install the latest patches for your system, servers and applications to protect them from the latest virus, malware and threats. Monitor your network traffic and block attempts to exploit your server and network by cyber-attackers.

CHANGE YOUR PASSWORD

We highly recommend to change your passwords regularly, such as every 90 days. Change your password immediately if you think your password has been compromised or if your login credentials have been stolen.

CONNECT SECURELY

Use Virtual Private Network (VPN) connections to securely access your internal resources or when you're dealing with sensitive information. VPN allows you to access your local network resources securely from anywhere in the world even when using public hotspots and prevents others from snooping on your network traffic.

ENGAGE WISELY

Do not visit any untrusted websites and refrain from opening any links, attachments or emails to mitigate the risk of a cyberattack. Attackers tend to lure users to click on a link or open an attachment, so verify any information received from emails, text messages and social media posts. At the same time, block malicious emails with subjects and hashtags related to trending topics, for example, Coronavirus or COVID-19.

SAFEGUARD YOUR IDENTITY

Be careful and verify any calls or emails claiming to be from legal enforcement agencies, banks or companies that you may have dealings with. Do not simply divulge information regarding your identity over any unverified calls, or enter personal information, such as email address or password, whenever you are requested to do so on a website or an email. Do the same for your customers by safeguarding their identities with one-time password solutions such as BOLD.Key for secured authentication and verification in your business transactions.

KEEP UPDATED

Check for the latest update releases for applications on your mobile phone as well as security updates on your computer's operating system regularly. Apart from fixing bugs, these updates help to identify the latest threats and keep potential cyberattacks at bay.

USE SECURE SOLUTIONS

If you're incorporating a payment feature in your business, it's important to choose a trusted payment platform that ensures peace of mind for both buyers and sellers. BOLD.Pay's dynamic payment solution is certified and licensed with solid processes and procedures in place such as pay-out policy, refund policy and service level agreements to minimise the risk of fraud.

MAKE A REPORT

You are advised to immediately contact the relevant law enforcement agencies if you suspect you have been the victim of a scam. Report any cybersecurity incidences to your country's respective Cyber Security Agency if your server has been breached, compromised or defaced.

For service and support of MACROKIOSK's solutions, please direct it to our dedicated business consultant, contact us directly through the official contact details published on our website or call our Technical Support Line (operates 24 hours a day, 7 days a week).