# Cyber security newsletter

October 2018

## Be careful when downloading apps!

Apps provide a world of wonderful capabilities for your device, but they are also a way for malicious actors to disseminate malware or gather information about you. Only use app providers you can trust - Google's Play Store and Apple's App Store proactively remove known malicious apps to protect users. Be proactive - read privacy statements, review permissions, check reviews and look online to see if security companies have identified an app as malicious before you decide to download it.

## Avoiding malware

Every time we use our devices, browse the Internet and open emails, we are potentially exposing those devices to malicious software (malware). Malware is software designed to damage or allow unauthorised access to devices or networks. Malware comes in many different forms, all of which have negative effects. With a little extra vigilance, and some good habits and practices, you can greatly reduce your chances of being infected by malware and can minimise the impact on your device, data, and life if it does become infected.

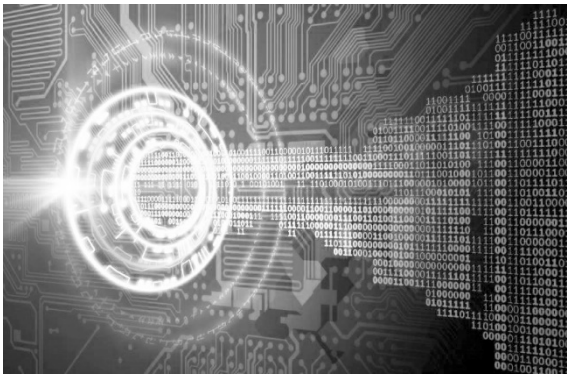
## Common types of malware & their effects

Ransomware – Ransomware is malware that stops you from being able to access your files, usually by encrypting them, and then requests payment to decrypt the files, restoring your access. Payment is usually requested in bitcoin, a popular, non-traceable cryptocurrency. Unfortunately, paying the ransom does not guarantee restored access to your files.

Trojan horses (a.k.a. trojans) – This malware takes its name from the classic story of the Greeks sneaking soldiers into Troy, hidden inside a large wooden horse. Trojans behave in much the same way, by appearing to be legitimate apps or software. Some trojans allow an attacker full access to your device, others steal banking and sensitive information, and others are simply used to download additional malware, like ransomware.

## Tips & practices to avoid - or survive - malware

Update and patch your devices and software - Vendors release updates and patches to fix security issues, not just to fix functionality! Many types of malware can be foiled by keeping your software up-to-date by accepting updates when notified about them.



Never click suspicious or untrusted links - Even if a URL comes from a company or person you know, it is always safest to manually type URLs into your browser. If nothing else, hover over the link to discover where it's really sending you, as malicious actors often send convincing-looking emails. This advice is also true for links in emails, documents and on social media platforms.

Download from trusted sources -- When looking to download an app or software, only do so from a trusted vendor or source. On mobile devices, ensure that you only download apps from the Google Play store or Apple's App Store, which are trusted sources for Android and iOS devices.

Back up your data - and ensure backups are good! Backing up your data, whether by doing a complete backup of your whole device or just key files, is the best way to protect those important files and pictures against ransomware and other data loss.


Contact us:

Srikant Ranganathan
Senior Director
IT consulting
+973 1720 6827

Mohammed Al Meftah
Senior Consultant
IT consulting
+973 1720 6834