Digital Jewels
information value chain consultants
PCI DSS QUALIFIED SECURITY ASSESSOR
ISO/IEC 27001:2013 (ISMS) CERTIFIED
ISO/IEC 9001:2015 (QMS) CERTIFIED

CYBERSECURITY AWARENESS MONTH

STAYING SAFE ONLINE

Hello,

It is cyber security awareness month 2020 and a great time to learn how to stay safe online!

As more and more of our data and lives are stored and spent online, it is very important that we understand how to protect both our devices and our information from malicious elements online. Leaving devices unprotected can result in anything as small as a slower computer (not so small if you have pending deliverables and a deadline coming up), right through to losing all the money in your bank account, to identity theft.

Outside of your online banking, people need to pay considerable thought to protecting their information. There are several ways they can easily go about this to ensure some level of security is achieved.

What are the best ways to stay safe?

PASSWORDS- One of the easiest ways to protect yourself online is to improve your password protection. It was recently shown that the most common password in the world is 123456. So if that's your password, it is advisable that you change it right away! Here are just three easy steps to improve your password:

- Use numbers, characters and a mix of lower-case and capital letters in your password
- Avoid using anything personal about you in it
- If you cannot remember your password, use a password manager to help you keep a record of complex passwords

USE ANTI-VIRUS SOFTWARE --These are designed to take a lot of the load off of your shoulders, protecting you from the less obvious malware that may make it past the untrained or unfamiliar eye. There are plenty of trustworthy programs available, some at cost and some free to use, such as AVG's basic version, it's up to you to decide what best suits you and your needs.

UPDATE REGULARLY-- It's not enough to just have virus software, you need to keep it up to date. Malware is constantly changing and evolving, so you have to do the same. Update any software you use regularly as well, as developers often improve the security of their software after release as problems and new malware emerge.

KEEP ABREAST OF THE TRENDS

Further to taking the steps above, do your best to develop your knowledge, try to stay on top of current trends in malware and have an understanding of the kind of sites that put you at risk. Some of the biggest offenders include:

FLASH SITES-- Flash sites use cookies ,small bits of data used to track your location. These are easily exploited by malware and as a result are vulnerable. The best thing to do is to avoid these sites entirely, but if you do use them, make sure that your flash is up to date to protect you as much as possible.

SHORTENED URLS- shortened URLs are very popular, but they can be used to disguise malicious websites. If you don't trust the source of the URL, don't click it.

MODIFIED URLS- Hackers take advantage of the fact that people may ignore certain modifications to a URL - for instance, a visitor may be directed to visit a 'twiitter.com' website instead of 'twitter.com'. All activities logged on could be monitored and credentials stolen from an un-suspecting user. For this reason, you should always be sure to check any URLs to which you are linked from an unknown or untrustworthy source.

EMAIL- A lot of us think of our email as safe, but we can still be subject to a cyber-attack there. Email attachments can often disguise malicious software that can install itself on your computer as soon as you open it. Most email clients have pretty sophisticated junk filters, but the occasional one can get through, so keep an eye out for suspicious emails and their attachments.

PUBLIC WI-FI- It's not a website but using public Wi-Fi can put you at risk because it opens your computer up to anyone else using the Wi-Fi if it's unsecured. If you're using public Wi-Fi we advise you refrain from accessing any sensitive information, such as online banking or logging into sensitive work documents.

You owe it to yourself to exercise some level of caution and stay safe online.

Do Look forward to more cybersecurity tips from our team on our social media pages.

Feel free to share your experience, or leave a comment on this subject of staying safe online