AUCAMP INC

ATTORNEYS, NOTARIES, CONVEYANCERS

Cybercrime

AUCAMP INC

ATTORNEYS, NOTARIES, CONVEYANCERS

Cybercrime

There has been an increase in reports of email hacking scams involving the theft of money intended to be paid as the purchase price of property, transfer costs and fees.

In most of the incidents reported, the hackers gained access to the email accounts of the seller or the purchaser. The hackers use the email addresses of these parties to communicate fraudulent banking details. Parties are usually unsuspecting as they expect the emails and the emails form part of an existing chain of correspondence.

The unsuspecting victim ends up paying the fraudster instead of the intended recipient. Life savings can be lost through these scams as the fraudulent accounts are usually cleared by the time that the crime is discovered. With property transactions, where there may be a whole team working on each side, the risk is perhaps greater: more people to unwittingly disclose information.

THE FOLLOWING STEPS CAN HELP TO STOP YOU BECOMING A VICTIM OF CYBERCRIME:

1. Restrict the disclosure of bank account details and limit the number of people able to authorise bank account payments/transfers.
2. Ensure your computer is protected by security software and keep it updated. Use encrypted emails and password protected portals. If your anti-virus programmes are not constantly updated they are of no use.
3. Resist the temptation to announce future property transactions online (via social media or your website), for example that you will be moving to a new office building or taking on more premises. Wait until after the transaction has completed.
4. Avoid communicating sensitive information like bank account details by email, as it could be intercepted by hackers. Do so in person, by secure letter, or by telephone if you know the person you are talking to.
5. If someone you do not recognise calls to discuss the transaction, tell them you will call back. Then try to figure out whether they are genuine e.g. if they say they are from one of the organisations involved, contact someone you know there to check.
6. Look out for fraudulent emails:
7. Check the sender's address by clicking the "reply" option (but do not reply). It might turn out to be different from the address that appears in the "from" box. A business email address usually incorporates the business name. Be suspicious if the address is from a free email account provider like Hotmail, Gmail, Yahoo.
8. If you become suspicious that your may be the target of cyber criminals alert those acting for you in the transaction. If there is no innocent explanation for the suspicious behaviour, contact the police.

Types of cybercrime

Identity theft
Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains. When this is done online on the Internet, its is called Online Identity Theft.

Ransomware
This is one of the detestable malware-based attacks. Ransomware enters your computer network and encrypts your files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this private key.

DDoS attacks
DDoS attacks are used to make an online service unavailable and bring it down, by bombarding or overwhelming it with traffic from multiple locations and sources. Large networks of infected computers, called Botnets are developed by planting malware on the victim computers.

Spam and Phishing
Spamming and phishing are two very common forms of cybercrimes. There is not much you can do to control them. Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cyber criminals offer a bait so that you take it and give out the information they want. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, and anything that promises you money for nothing or a small favor.

Social Engineering
Social engineering is a method where the cyber criminals make a direct contact with you using emails or phones – mostly the latter. They try to gain your confidence and once they succeed at it, they get the information they need. This information can be about you, your money, your company where you work or anything that can be of interest to the cyber criminals.

Remote Administration Tools
Remote Administration Tools are used to carry out illegal activities. It can be used to control the computer using shell commands, steal files/data, send location of the computer to a remote controlling device and more.

Preventive steps against Cybercrime
Apart from inculcating safe browsing habits, maintain good system hygiene. Avoid leaving Digital Footprints. You must secure your Windows system with a fully updated operating system and installed software, and ensure that you install a good Internet security software to protect your Windows 8.1 computer. Using the Enhanced Mitigation Experience Toolkiton Windows is a great way to protect your system against zero-day attacks.

EXTREMELY IMPORTANT: OUR OFFICE WILL NEVER CHANGE OUR BANKING DETAILS WITH NOTIFICATION TO YOU VIA EMAIL OR ANY OTHER ELECTRONIC COMMUNICATION. WE WILL NOT BE LIABLE FOR ANY LOSSES SUFFERED AS A RESULT OF THE COMPLIANCE WITH ANY FRAUDULENT INSTRUCTION TO AMEND BANKING DETAILS.