Electronic Crime (E-Crime)

Increasingly, retailers that businesses use for goods and services are opening their business and telephone lines to customers and suppliers through electronic trading. Coupled with the many benefits that electronic trading provides, it can however expose an organisation to unique methods of crime involving the organisation, suppliers and customers.

How can I protect my Organisation?

It is important to put in place some measures to reduce risk and protect your businesses information.

Prevention

Basic Security Tips

1. Install reputable anti-virus software and keep it up-to-date.
2. Install reputable firewall software and keep it up-to-date.
3. Keep software patched up-to-date.
4. Passwords should be confidential, complex and regularly changed.
    - Immediately remove internal/external network access of staff/volunteers leaving employment for whatever reason
    - Where you suspect that your network/access password has become known to a third party, change it immediately
    - Do not leave your computer logged in to the network whilst you are not present (log off or lock your computer)
    - Where possible consider setting a short time out on your screen saver and ensure that log-in is required to recover from the screen saver.
5. Delete any suspicious emails without opening - curiosity is a tool often used to hack a computer system or send a virus.
6. Do not open email attachments which have not been scanned for viruses/ malware, or have been received from an unknown source.
7. Only download software from reputable sources.
8. Backup critical data and keep it separate from your Internet connected computers. Regularly copy the data to a CD or other backup device.
9. Test that you can recover the information using that backup device.

How do I know if my Network has been hacked?

The following is a useful list of potential indicators which may indicate the presence of hackers within your network/ computer system.

1. Your website has been changed.
2. Your computer system performance is unusually and exceptionally slow.
3. Your antivirus software does not appear to be functioning or has been disabled.
4. Confidential information on your businesses activities have been exposed to the general public.
5. Transactions have been changed eg: a client or supplier account which had a balance of $1,000 now has $950 without your authorisation.
6. Your website/ server logs have been deleted
7. There is odd activity in a computer log and the more it's investigated the more you suspect that something is wrong.

8. Established business procedures do not appear to have been followed and transactions are unexplainable. This may indicate that someone is operating outside of your control and using your system.
9. You are no longer receiving emails and no-one receives emails you have sent.
10. You can no longer access Microsoft Word, Excel, Powerpoint or PDF documents.
11. The entire system shuts down.
12. There is a new program on your computer that you didn't install. Your password has been changed and/or you can't access your network. There is an unexplained large increase in web traffic to your website.

Online Fraud

If you believe that you have been the victim of an online auction fraud, immediately report the matter to the auction company (i.e. eBay). Most online auction houses have an identified process for reporting following-up suspect transactions and can often assist you with recovering your property and providing you with records that you will require to report the matter to the police, if a crime is identified.

If you become the victim of on-line fraud, report the matter to your local police. Ensure that you preserve any electronic evidence (logs, emails or other communications between yourself and the suspect) relating to the matter. If you are confident in the process, create an electronic copy of each email including all header information, and burn it to a CD or DVD. Do NOT delete the original emails. When reporting the fraud ensure that you provide a copy of the CD or DVD to the police.