CYBER SECURITY GUIDE

Purpose:
It is the duty of our Company to train, promote and enforce Cyber security and Communications, ensuring clear Rules and Codes of Conduct are established and adhered to, regarding the operation and use of IT equipment, systems and platforms, with the intention of creating a Professional, Secure and Intelligent environment. This guideline will define both as a Business and those expected from every Employee. We will clearly with Best Practice create ideas to help provide a safe and stable environment that is protected against Cyber security and Cyber threats to the business.

Scope:
This Cyber security guide applies to all Employees of Advantage One Security, including the extension of your responsibilities outside of work. This Guide covers the use of Personal, Customer or Company equipment and systems, including the use of phones, computers, tablets or smart-phones, or any system capable of operating; Internet, Customer Reporting systems, Social Media, Email, Telephone Calls, A.I.P., IT Networks and general computing & communication systems.

Failure to comply with the rules set out in the Cyber security Guidance: may lead to disciplinary action being taken against you, including dismissal

This Guide contains information on:

1. What is cyber-crime:

Cyber is the communication between computers and all things web based in short, cybercrime is any type of illegal activity that takes place via digital means. Data theft is, of course, one of the most common types of cybercrime, but cybercrime also includes a wide range of malicious activity as well, such as cyberbullying or planting worms or viruses. Cybercrimes can be divided into two distinct categories: those that cause intentional damage and those that cause unintentional damage. In most cases, the damage is financial but not always.

2.Types of Cyber-crime:

Hacking: Hacking is simply any unauthorized access of a computer system. Sometimes, hacking can be fairly harmless, such as rewriting sections of an existing software program to allow access to features the original designer did not intend. While this is technically a violation of the Terms of Service agreement, it is not exactly a prosecutable offense but is still considered hacking. Hacking is probably one of the most broadly used forms of cybercrime, but not all hackers are criminals. Some hackers often referred to as "white hat" hackers, are hired by software companies to find flaws in their systems so they can fix them before "black hat" or criminal hackers do.

Viruses, Worms, Malware and Ransomware: Many types of malicious software can be delivered by a wide range of means. In the case of most viruses, they need to actually be downloaded in some way onto a hard drive. In targeted attacks, a victim may receive an innocent-looking email that is ostensibly from a co-worker or trusted individual containing a link to click on or file to download. In other cases, websites may contain infected links that download worms or viruses when you click on them. In some cases, they are disguised as banner ads that actually deliver malware as soon as you click on the link.

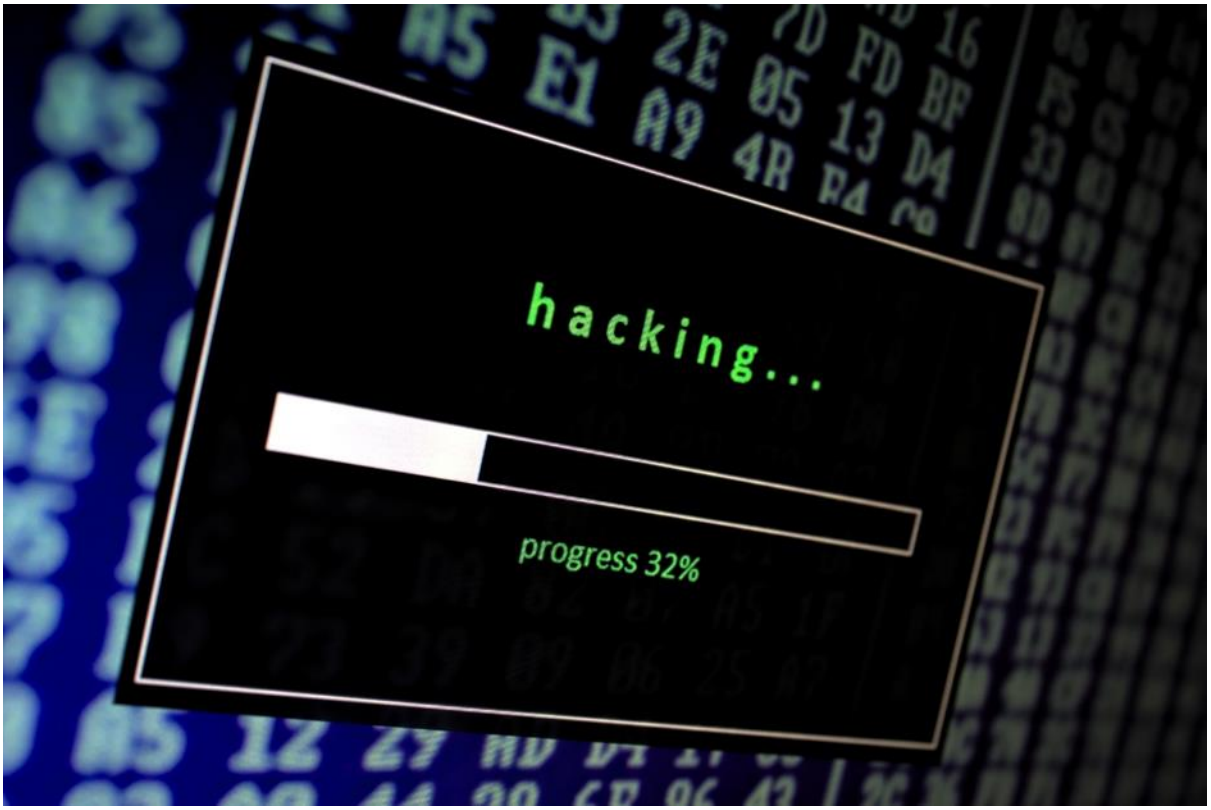
Denial-of-Service (DOS) attack, Email bombing or spamming: These types of attacks flood systems with so much information that it can crash the servers that cyber businesses depend on. A DOS attack, for instance, sends a flood of fake traffic to a website, which overloads the server, causing a website to temporarily malfunction or in some cases, crash completely. DOS attacks can also be committed strategically to interfere with a specific event that can cause a financial catastrophe. For instance, when concert tickets for a certain artist go on sale, a DOS attack can keep anyone from buying tickets and possibly even crash the site. In that case, they don't just cause a massive financial loss to the ticket seller, but also to the artist.

3.Types of Cyber Security Threats:

There are a wide variety of cyber security threats. More are popping up every day. Here is a list of the most common types of threats.

- Adware
- Browser Hijacker

- Data Breaches
- Identity Theft
- Password Attacks
- Phishing E-mails
- Ransomware
- Spyware and Keyloggers
- Trojans
- Worms
- Viruses



4.Emails:

Communication via Email is a vital method for everyone, including Businesses, to pass information between each other, quickly and easily. Email should be treated in the same way as all formal written correspondence and the same standards of behaviour apply.

- Advantage One Security's email system is primarily for business use. Misuse may lead to disciplinary action and may in certain circumstances be treated as gross misconduct.
- All email is stored and email may be subject to monitoring for security, verification of this Guidance and/or network management reasons by the company at any time without notice.
- Obtain confirmation of receipt for all important external emails sent.
- Keep all passwords secure. All passwords used on Company computers/laptops must be registered with the Office Manager.
- Do not visit, view or download any material for any Internet website containing sexual or illegal material or material which may result in downloading a virus.
- Do not subscribe to any bulletin boards, groups etc. without prior permission of the Operations Director.
- Do not download software onto the company's network system or laptop computers without prior permission from the Operations Director. This includes software and shareware available for free on the internet.
- Do not load any file or material onto a company computer/laptop
- You must not intentionally interfere with the normal operation of the network.

- You must inform the Operations Director should you detect or suspect a computer virus in any file, email or attachment on your computer, immediately.
- Use of social networking sites via Company computers is not permitted.

5.Best practice (Do's):

- Use secure passwords
- Change your passwords regular (Ask company Management to keep this updated)
- Use different passwords for different sites requiring passwords
- Only send data to entrusted emails
- Be wary of links you receive from emails Report any links to your line manager

6.Best practice (don'ts)

- Use personal USB sticks in company property
- Save any personal data on company I.T
- Save any Password's on company I.T
- Download data to company I.T
- Connect to untrusted web pages (Social Media i.e., Facebook)
- Click on unknown Hyperlinks
- Give out personal or company Details to untrusted sites
- Send or receive data from Company I.T to a personal account
- Reply to malicious emails
- Upload pictures from personal phone to company I.T equipment
- Install apps on company I.T Equipment
- Don't provide personal information on line to get something for free
- Do not click on links inside unauthorised emails

Failure to comply with the rules set out in these Cyber security Guidelines: may lead to disciplinary action being taken against you, including dismissal