# Small Business Security Guides

## Cyber criminals and who to protect against

AVG AT WORK

# Five steps to securing your business website and its content

Today, almost all computers are connected to the Internet. This means they're connected to other computers – which involves risk.

We use our PCs for both work and play. We shop, bank and play games online – even when we're at work – but we also work when we're at home. The web is a research tool and an entertainment centre, letting us access music, movies, TV shows and much more. In doing so we store useful information, indeed even vital private and personal information on our PCs.

Therefore, it is extremely important that you store your information properly and keep it secure. It's also important that you protect your PCs from misuse, abuse and data loss. Why? Because there are bad guys out there trying to get their hands on your information.

Bad guys? Yes, it's a term we use frequently, but do you fully understand who the bad guys are?

Before you can properly arm yourself against a security attack and/or breach by the bad guys, it helps if you know who to watch for so that you can put in place the proper layers of defence.

There are actually quite a few unique categories of bad guys to look out for. They are variously referred to as hackers, crackers, script kiddies, cyber criminals, cyber spies, cyber extortionists, cyber activists, cyber terrorists, cyber warriors, and even unethical friends or staff. Technically a cyber crime is any intentional breach in computer security via the Internet, or some other illegal act facilitated by the Internet.

# Business basics: Definitions

### Hackers

There was a time when "hackers" wore white hats. They illegally accessed computers to learn more about them, or to find security holes in the computer or the network to which it's attached. They did nothing malicious and took pride in the quality of hacks that would leave no trace of an intrusion.

### Crackers

Then the hacking landscape changed and we started to see a dominance of crackers" – people who intentionally accesses a computer, or network of computers to cause harm, inflict damage or steal data. Usually, both hackers and crackers have very advanced computer and networking skills allowing them to develop scripts or programs to help them attack computer systems and networks.

### Script Kiddies

Hacking tools can sometimes end up in the hands of "Script Kiddies", who then use them, often randomly and with little regard or understanding of the consequences. Script kiddies often have limited skills and can be quite immature, often trying to effect large numbers of attacks in order to obtain attention and notoriety.

### Cyber Criminals

We typically use the term "cyber criminal" to describe someone who uses the Internet in illegal ways, or to facilitate illegal or fraudulent activities.

More specifically, cyber criminals are the people trying to place malware on your system so they can obtain valuable information such as credit card and bank account details, usernames and passwords. This is identity theft and those responsible will either use the information to defraud someone, or sell it on to someone else who will.

Cyber criminals are also scammers and phishers who try to con you into giving them money. They might ask you to transfer large amounts of money, or tell you that you've won a prize in a lottery you never entered. Sometimes their scam is the promise of an inheritance from a wealthy relative you've never heard of.

Some cyber criminals illegally distribute software, music, movies against copyright laws. They might even sell illegal forms of pornography. Typically their activities are entirely profit motivated. Though in the cases of cyber bullying and cyber grooming the motivations lie elsewhere.

Not all cyber criminals have sophisticated computer and networking skills. Today, the vast majority of cyber criminals simply use the malicious tools and kits marketed for profit by those creating them.

So most cyber criminals are simply up-to-date Script Kiddies, but now they're motivated by profit, not notoriety. For about US$400, almost anyone can buy appropriate scripts and after about four hours of following  the instructions be fully setup as a cyber criminal. Scary stuff.

### Cyber spy

Typically someone trying to obtain information about companies or government organisations. Typically when the attack is against a business it is profit driven, while when it's against government organisations it is international espionage.

# Business basics: Definitions

### Cyber extortionist

Someone who carries out blackmail via the Internet. For instance, threatening to release confidential information if an individual or company does not pay a large amount of money. Cyber extortionists may put in place a distributed denial of service attack (DDoS) against the website or network of a business and demand payment to stop the attack. They might trick you into downloading and installing malware/scareware/scamware, such as rogue anti-virus software, and then demand payment to remove it.

### Cyber activist

Someone who uses the Internet to enable faster communications to help organise public demonstrations, sometimes related to fundraising, community building, lobbying and organising. One example is Iranians using Twitter to organise mass protests in 2009.

### Cyber terrorist

This is a cyber criminal who uses the Internet to destroy computers or disrupt Internet connected services for political reasons. Just like a regular terrorist attack, cyber terrorism typically requires highly skilled individuals, a lot of money to implement, and detailed planning. An example is when hundreds of DDoS attacks in 2007 virtually took down the Internet in Estonia.

It seems that many countries, including the USA and China, have decided that the Internet is a valid tool to fight a war against their enemies. While the Internet can be used to greatly enhance military and economic power, it also presents a soft underbelly to present and future adversaries. Thus governments are recruiting and training cyber warriors to use the Internet for offensive attacks, and to protect us from such attacks by others. Sad, but true.

By going online, everyone is exposed to the bad guys. Thus it's crucial for both businesses and individuals to keep their information secure so that the bad guys can't gain access to it.

### How to protect your business and yourself

- Get up-to-date and properly configured Internet Security software on all PCs you use, like **AVG Internet Security Business Edition 10**
- Understand who might be looking to break through your defences and how they might do it. Hopefully the information we've provided here will help you to do this.
- Watch this video to see how AVG protection has helped these businesses

AVG SMB group at:
bit.ly/AVGSMB

Become an AVG Fan at:
facebook.com/avgfree

Read our blogs at:
blogs.avg.com

Follow us at:
twitter.com/
officialAVGnews

Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

AVG AT WORK