

AVG Community Powered Threat Report - Q1 2011

Contents

AVG Community Powered Threat Report - Q1 2011.....	1
Introduction	3
Key Points – Q1 2011.....	4
Quarterly Key Metrics: January – March 2011.....	5
Metrics -Web Threats	5
Top 10 Web Threats Prevalence Table Q1 2011	5
Top 5 Social Engineering Prevalence Table Q1 2011	5
Top 10 Malware Threat Prevalence Table Q1 2011	6
Behavior Categories Chart Q1 2011	6
Top Toolkits Seen in Q1 2011	7
Most Active Malicious Domains Q1 2011	7
This table shows a list of domains that caused the greatest percentage of global detections	7
Metrics - Mobile Threats.....	7
Top Malicious Android Applications Q1 2011	7
Metrics - Email Threats	8
Top 10 Domains in Spam Messages Q1 2011 Top 5 Languages in Spam Messages Q1 2011	8
Top Countries of Spam Senders Q1 2011 Top ISP's in Spam Messages Q1 2011	8
Web Risks & Threats.....	8
Rash of Facebook Attacks	8
Mobile Devices Risks & Threats	10
About AVG Technologies	11



Introduction

The AVG report is based on the Community Protection Network traffic and data followed by research performed by AVG, over a three-month period. It provides an overview of web, mobile devices, Spam risks and threats. The statistics referenced are obtained from the AVG Community Protection Network.

AVG Community Protection Network is an online neighborhood watch, helping everyone in the community to protect each other. Information about the latest threats is collected from customers who choose to participate in the product improvement program and shared with the community to make sure everyone receives the best possible protection.

With more than 120 million users using AVG's various solutions, AVG provides strong community protection. Each new user who chooses to participate increases the security level of all of us as a whole.

AVG has focused on building communities that help millions of online participants support each other on computer security issues and actively contribute to AVG's research efforts.

Q1 2011 Highlights

Web Threats		
▲	10.60%	Increase in global detections
	BlackHole⁽¹⁾	The most active threat on the Web, 44.20% of detected malware
	BlackHole	The most prevalent exploit toolkit in the wild, account for 86.68% of toolkits
▲	51%	Toolkits account for 51% of all threat activity on malicious websites
	11.33%	Of malware are using external hardware devices (e.g. flash drives) as a distribution method (AutoRun)
Smartphone's Threats		
	DownloadManagerExploit	The most downloaded malicious android application
	0.22%	Of Android applications are malicious
	0.02%	Of SMS sent from smart phones are malicious – 3.75M in US alone
Messaging Threats (Spam)		
	United States	Is the top Spam source country
	40.72%	Of Spam messages were originated from the USA followed by the United Kingdom with 5.87%
▲	bit.ly	Is the most exploited URL shortening service which is abused to spread Spam messages
	English	Is the top language used in Spam messages

(1) BlackHole Toolkit is an attack toolkit, that exploits several vulnerabilities (among them zero-day vulnerability) to execute arbitrary code. Attack toolkit is popular among criminals that buy it for use in their operations.

Key Points – Q1 2011

The trend in Q1 2011 could be characterized as “more” rather than “new”. What this means is that we saw increased, but not innovative, cybercriminal activity. This is a natural consequence of a maturing market, and we should expect to see this trend continue in Q2 2011. Cybercrime is growing and will continue to grow with great financial success for the criminals behind it.

Even though there were no remarkable new developments, it’s worthwhile to list the major increases in current attack techniques.

- (1) **Facebook PUS.** The biggest increase we noticed is the organized attempt to profit from Facebook’s growing popularity and adoption. It might be a bit extreme, but not too far from the mark when we call these sites PUS (Potentially Unwanted Sites). These sites typically lure victims by pretending to offer a “seedy” or perhaps morbid video with a titles such as “OMG, you won’t believe what this teen did on camera” or “OMG, you won’t believe what this teacher did to this student.”

Victims try to view the video, but instead of seeing it, they are asked to “prove they are a human being” by filling out a survey. Unfortunately, they never get to see the video, and are instead asked to fill out survey after survey. At some point, they are asked for their cell phone number, and are sent a text, to which they need to respond. If you read the fine print, the text response actually agrees that their cell phone should be charged \$9.95 per month. We expect that they catch lots of teens whose parents just pay the cell phone bill without noticing the extra \$10 per month.

Very often, one of the survey pages includes click-jacking or so-called like-jacking. The attack page asks the victim to press a button, but although it’s not visible to the viewer, the attack page has placed a transparent GIF over the top of the button, so that instead of the button getting the click, the GIF gets it. This is known as Click-jacking (high-jacking a click) or Like-jacking, and the GIF then runs a script to tell all your Facebook friends that you “like” this video, and that they should try it. In this way, they take advantage of the viral nature of Facebook to spread.

Last year, we used to see an average of one such campaign per week, usually running on weekends, and usually netting 200k-300k victims, but this has now accelerated to a fresh campaign every other day or so.

- (2) **Increased Blackhole activity.** Blackhole Exploit Kit is a relatively new kit that we wrote about recently, having first been detected in the 3rd or 4th quarter of 2010, but in February 2011, Blackhole was used in a huge and highly coordinated attack, largely targeting the UK. To give some numbers, Blackhole suddenly went from just a couple of hundred detections per day to a couple of hundred thousand per day in the course of just a week in February, and then on a couple of days, peaked at a massive 800k detections per day.

Interestingly, most of those detections seem to have originated from a combination of ad networks and adult sites, but most interestingly, they were targeting the UK more than anywhere else.

Another noteworthy aspect of this was that more than 600 attack servers were used in the attack, mostly based in Latvia. These were not hacked servers, but were rather servers that were deliberately brought online for just a couple of weeks for this attack.

This demonstrates the professionalism of the attackers who were able to bring 600 servers online at the same time as they launched attacks through ad servers and selected adult sites. This would have required significant capital investment and significant coordination and planning, and speaks to the sophistication and financial strength of the attackers.

- (3) **Soaring Android malware – mainly from China.** Android OS accounted for 22.7 % of worldwide Smart phone sales (source: Gartner.com).

As our experience tells us, hackers will be where people are, and as more and more people are purchasing an Android powered smart phone, it is not surprising to find the number of malware soaring in geographic where Android takes market share.

The open source nature of the OS as well as the open-garden approach in allowing users to install software on the mobile device *open the door* for hackers to write their malicious code. The fragmentation of the Android platform means that, even if Google fixes a vulnerability, not all users can or will update their OS. This is why Android users should use additional security solutions such as [AVG Mobilation for Android](#).

During the first quarter of 2011 we have seen a major increase in malware targeting Android smart phones. Some of these malware are legitimate pieces of software that were reversed engineered and malicious code was injected prior to a re-publishing of the binary on non-Google markets around the globe. These malware take advantage of users’ interest in the popular application for distribution.

Quarterly Key Metrics: January – March 2011

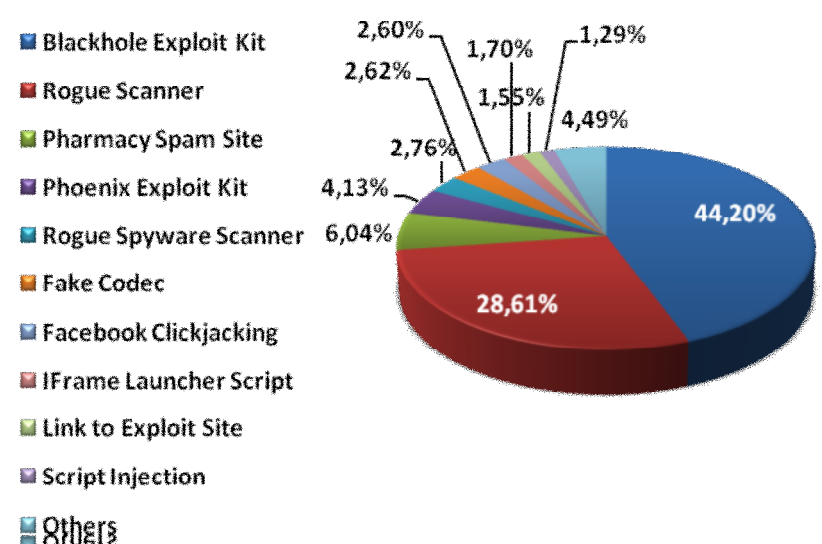
Metrics -Web Threats

Top 10 Web Threats Prevalence Table Q1 2011

This prevalence table shows top web threats as reported by Threat Labs Community

Blackhole Exploit Kit	44.20%	Pages containing script code characteristics of the Blackhole exploit kit, which is used to install a range of malware
Rogue Scanner	28.61%	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of apparently useful software
Pharmacy Spam Site	6.04%	The Pharmacy Spam sites appear to be legitimate online pharmacies, but usually are facsimiles of real sites. These fake pharmacies often supply generic, or even fake, drugs rather than the brands advertised, and reportedly often deliver no drugs at all
Phoenix Exploit Kit	4.13%	Crimeware toolkit which is used to install a range of malware
Rogue Spyware Scanner	2.76%	Pages containing fake anti-spyware scanners, or appear to be pages pushing fake anti-spyware products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of apparently useful software
Fake Codec	2.62%	Malicious Trojan disguised as a video codec
Facebook Clickjacking	2.60%	Facebook Clickjacking Worm
IFrame launcher Script	1.70%	Encrypted script used in malicious IFrames to launch exploits
Link to Exploit Site	1.55%	These pages contain links to known exploit sites. In some cases, malicious code is automatically downloaded without any user intervention
Script Injection	1.29%	Pages containing injected malicious scripts. Code injection can be used by an attacker to introduce (or "inject") code into a computer program to change the course of execution

Top 10 Web Threats Prevalence Chart Q1 2011

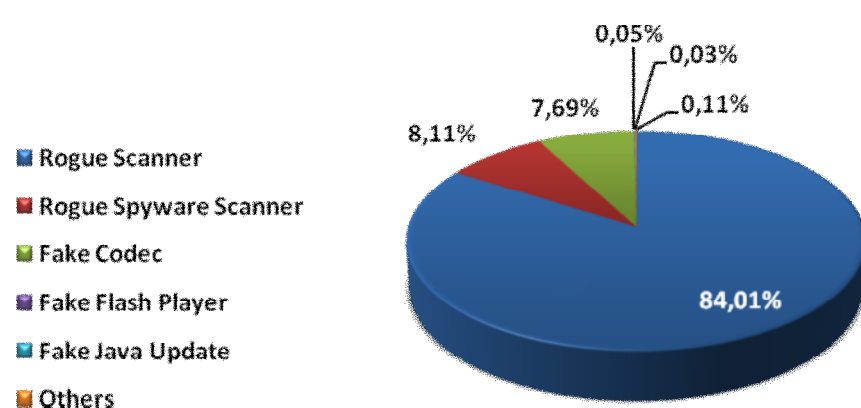


Top 5 Social Engineering Prevalence Table Q1 2011

These metrics present top Social Engineering techniques, which are used to lure novice users into installing a malicious program or disclosing private/financial information

Rogue Scanner	84.01%	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of apparently useful software
Rogue Spyware Scanner	8.11%	Fake Anti-Spyware Software
Fake Codec	7.69%	Malicious Trojan disguised as a video codec
Fake Flash Player	0.05%	Backdoor Trojan disguised as Macro Media Flash upgrade
Fake Java Update	0.03%	Trojan disguised as Java Update

Top 5 Social Engineering Prevalence Chart Q1 2011

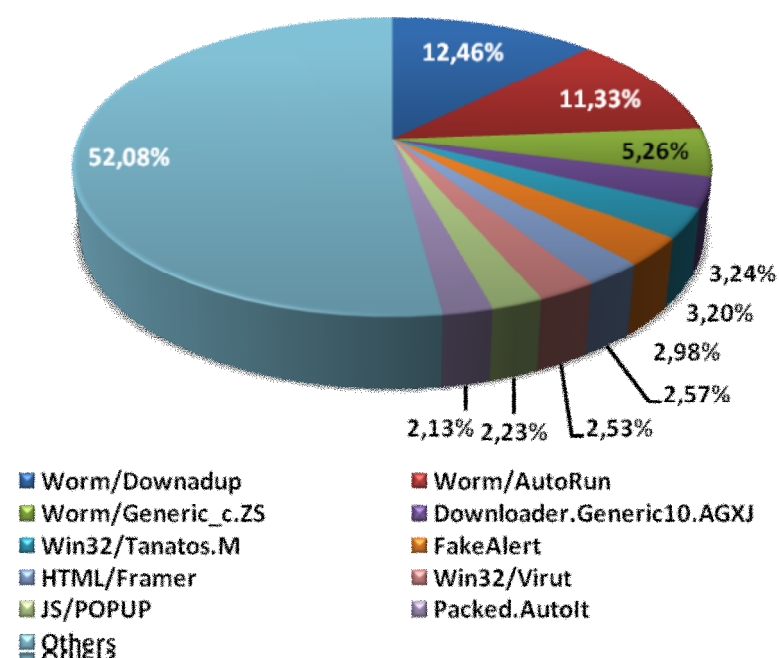


Top 10 Malware Threat Prevalence Table Q1 2011

This table presents top traditional malware as detected by AVG Threat Labs

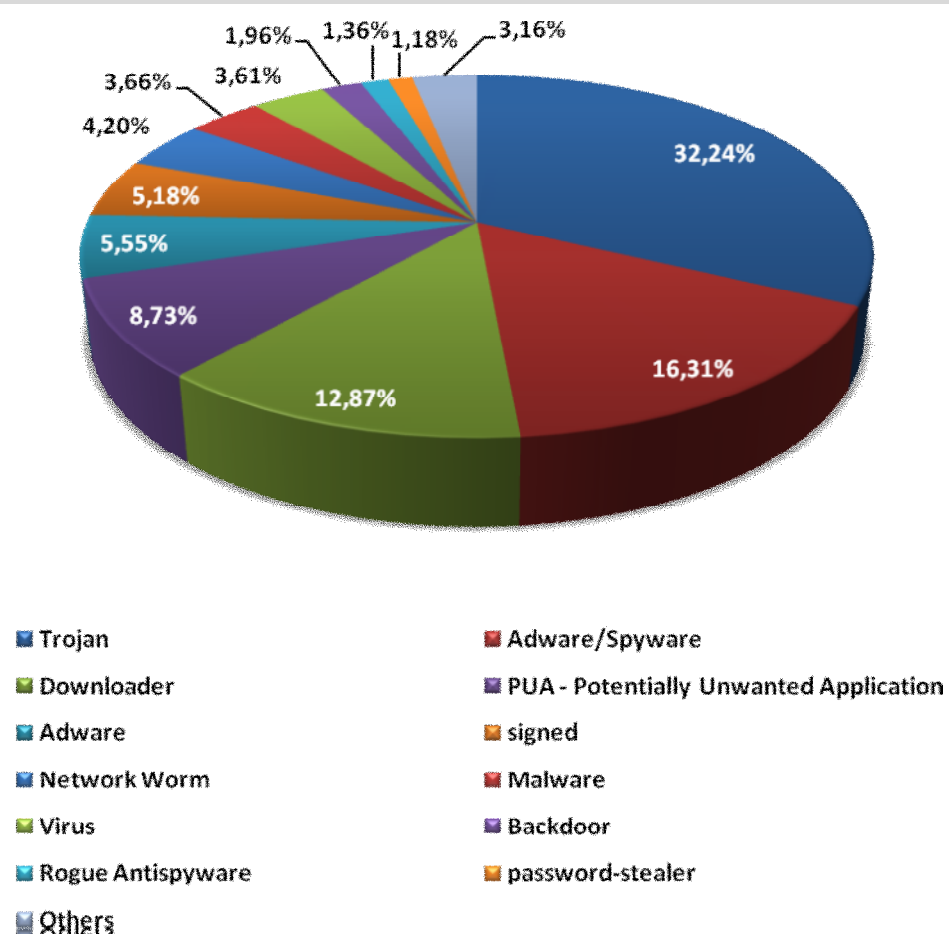
Worm/Downadup	12.46%
Worm/AutoRun	11.33%
Worm/Generic_c.ZS	5.26%
Downloader.Generic10.AGX	3.24%
Win32/Tanatos.M	3.20%
FakeAlert	2.98%
HTML/Framer	2.57%
Win32/Virut	2.53%
JS/POPU	2.23%
Packed.AutoIt	2.13%

Top 10 Malware Prevalence Chart Q1 2011



Behavior Categories Chart Q1 2011

This table presents threats prevalence as detected by AVG Identity Protection engine. This patent-pending technology looks at what the software does during execution. Using various classifiers and advanced algorithms, this technology determines the hostile behavior of files and prevents their execution





Top Toolkits Seen in Q1 2011

These metrics present the top five attack toolkits in terms of malicious web activities. Criminals are increasingly utilizing toolkits to carry on cyber attacks. In many cases, using attack toolkits does not require technical expertise

1	BlackHole	86.68%
2	Phoenix	8.10%
3	NeoSploit	2.10%
4	Bleeding Life	1.17%
5	Eleonore Exploit Kit	0.68%

Most Active Malicious Domains Q1 2011

This table shows a list of domains that caused the greatest percentage of global detections

1	t8good.info
2	antispym.com
3	btorik.info
4	sichuans.ir
5	pornoret.com

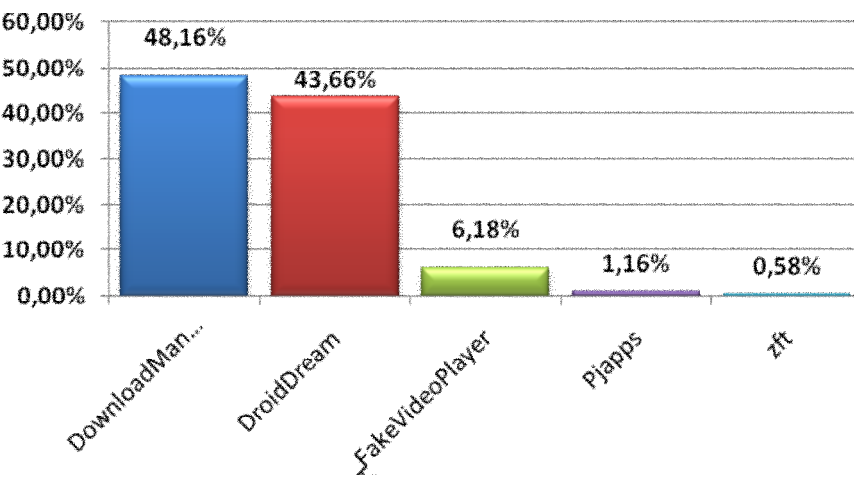
Metrics - Mobile Threats

Top Malicious Android Applications Q1 2011

This table shows the list of the top malicious Android applications as detected by AVG Threat Labs

DownloadManagerExploit	48.16%
DroidDream	43.66%
FakeVideoPlayer	6.18%
Pjapps	1.16%
Zft	0.58%



Top Malicious Android Applications Chart



Metrics - Email Threats






Top 10 Domains in Spam Messages Q1 2011

This table shows top domains used in Spam messages

1		t.co	5.02%
2		bit.ly	3.55%
3		durl.me	3.50%
4		hotmail.com	2.93%
5		yahoo.com	2.37%
6		viagra.com	2.06%
7		gmail.com	1.88%
8		Facebook.com	1.76%
9		tvescon.com	1.61%
10		twitter.com	1.54%

Top 5 Languages in Spam Messages Q1 2011

This table presents top languages used in global Spam

1		English	86.94%
2		Portuguese	3.01%
3		German	1.61%
4		French	1.54%
5		Chinese	1.40%


Top Countries of Spam Senders Q1 2011

This table shows top Spam source countries

1		United States	40.72%
2		United Kingdom	5.87%
3		Brazil	4.11%
4		Germany	3.50%
5		India	3.25%
6		Russian Federation	3.04%
7		France	2.11%
8		Ukraine	1.89%
9		China	1.89%
10		Italy	1.82%

Top ISP's in Spam Messages Q1 2011

This table presents top Internet Service providers that are used

1		Comite Gestor da Internet no Brasil	9.01%
2		Microsoft Corp	7.45%
3		3dgwebhosting.com Inc	3.79%
4		Postini Inc	3.52%
5		SingleHop	3.45%

Web Risks & Threats

Rash of Facebook Attacks

Finding and making friends online using social networking web sites such as Facebook has almost become a rite of passage. Today, Facebook is the second most popular site in the world according to Alexa's traffic rankings.

Facebook had explosive growth from 2008 with ~100 million users until today with ~520 million users which equates to about 7% of world's population or ~26% of global internet users; Facebook became the largest social network worldwide (source: usatoday.com)

Facebook's popularity has its price. Cyber criminals naturally tend to target the most popular applications or services used by the majority of Internet users, in the case of Facebook it can reach out to a huge amount of people. Social networks have become a haven for cyber criminals. The built-in trust among "friends" on social networks makes it easier for a cyber criminal to deploy successful attacks against these users.

Between 2008 - 2010, AVG has seen an exponential growth of Facebook related attacks per day.



In October 2010, AVG analyzed the safety of 50 global social networks and found that on the top 50 social network worldwide, there are ~20,000 compromised web pages, 60% of them are on Facebook. This piece of data alone should alarm Facebook fans and cause them to take precautions.

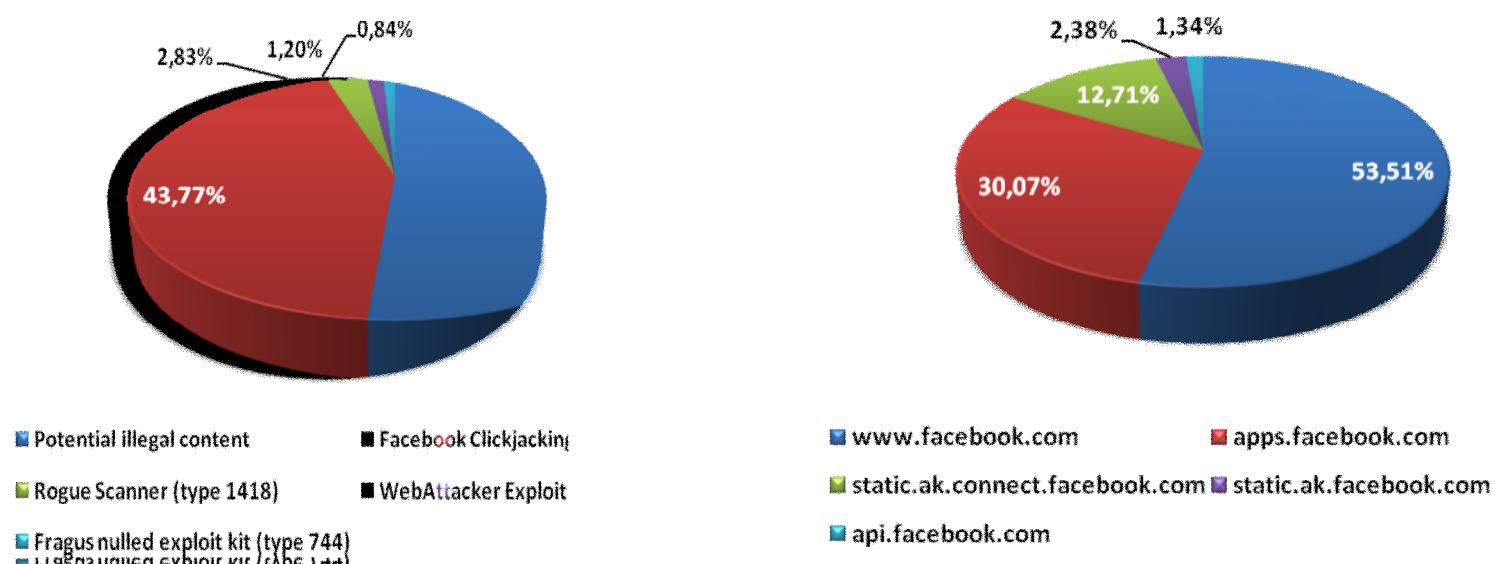
Content posted on Facebook poses a security risk to its users, based on our data.

AVG data also shows that ~42% of the detected malware on Facebook is related to Facebook's applications, combining this information with the fact that people on Facebook install 20 million applications daily (source: facebook.com), this poses a huge risk to Facebook users (individuals as well as corporate users).

People are at risk of losing control of personal information; users are not fully aware who can view their private information; the information could end up in the hands of marketers or cyber criminals. People should be careful of what application they should be using. They do not provide any private information to a stranger, but they easily share all their private information with applications on Facebook without fully knowing if it is safe or not, only because they do trust their friends who have done the same thing.

Identity theft is also a risk that people should pay attention to, by revealing so much information. Identity thieves can easily use people's identity in criminal activity and could also lead to losing credibility and/or reputation.

The risk is even bigger when adding mobile devices to the equation, there are more than 200 million active users currently accessing Facebook through their mobile devices (source: facebook.com). The risk here is not just trading personal data or identity theft, the risks of accessing the mobile device are stealing financial information, accessing all confidential information that is stored on the mobile device, accessing the corporate network, data leaks of corporate confidential information and so on and so forth.



Recommendation

- Check your privacy settings –make sure that your privacy settings aren't sharing information that you want to keep private.
- Pay attention to you share your information with.
- Protect your mobile device with a security tools same as you do for your PC or laptop.
- Use AVG Social Networking Protection: links that are exchanged within Facebook are automatically checked in real time so that you, your friends, your company, and your employees are safe. AVG Social Networking protection is activated automatically as soon as AVG is installed.
- It's great to use Facebook to keep in touch, to express yourself openly, and to find new friends, but **"let's be careful out there"**

Mobile Devices Risks & Threats

In 2010, global mobile phone sales totaled 1.6 billion units. Android accounted for 22.7 % of worldwide Smart phone sales (source: Gartner.com).

Gartner also forecasts that open OS mobile devices (Smart phones) will command 46% of all handset sales by 2014 and expects Android to play an important role in the media tablet market.

Parallel to the extreme growth of Android market share from 3.9% market share in 2009 to 22.7% market share in 2010 (source: Gartner.com), AVG have seen an exponential growth in malware targeting Android platform during 2010 especially during the 2nd half of 2010.



The sheer volume of cell phone users around the world indicates a current need for proactive mobile security measures. While more than 1.5 billion people use the Internet daily, over 4.5 billion use a cell phone every day, creating an attractive target for cyber criminals (Source: GTISC – Georgia tech information security center).

People have a false sense of security when it comes to mobile phones. A survey conducted by AVG and the Ponemon Institute (<http://free.avg.com/gb-en/news.ndi-166> , Feb 2011) among smart phones users revealed that more than a third of smart phone users are not aware of the increasing security risks associated with using their phones for financial purposes and to store personal data. The study also showed that just 29% of smart phone owners have considered downloading free or paid anti-virus software to help protect their most personal devices.

Smart Phone and Android in particular, pose a great risk for users, since mobile devices are constantly connected and substantially less protected than a personal computer as users shrug off mobile security solutions and carelessly broadcast financial, account and other personal data such as their exact location while on the go.

Smart Phones and Tablets are typically not equipped with the same security measures as PC & laptops.

With the growth of Android OS popularity due to its opened source nature, it provides fertile ground for hackers and cyber criminals to act. Attackers can take advantage of Smartphone users through email, Internet applications, Internet surfing and text messaging, etc.

Our research shows that during Q1 2011, 0.20% of downloaded Android applications are malicious.

Only recently Google removed applications from the Android market and remotely uninstalled malicious application from infected Smart Phones. Some of these applications tend to steal financial information.

According to androlib.com, there are ~307,000 applications on the Android Market (March 2011), this number was multiplied by ~30 since July 2009 (less than ~10,000 applications). According to androlib.com, ~3.9 Billion applications were downloaded, this means that potentially ~7.8 Millions malicious applications were downloaded. We expect to see a dramatic increase during 2011 and further.

Smartphone owners are exposed to threats from text messaging as well, our research shows that 0.02% of SMS sent are malicious, this seems like a low percentage and this might suggest a low chance to get infected BUT, in the USA alone, during Dec 2010, 187.7 Billion Text SMS were sent (source: www.ctia.org) which means that 3.75 Million messages are potentially malicious. The risk is higher than you might think at first.

Smart phones look more like the desktop world but unlike the desktop world, smart phone security levels are in its infancy, people's attitude to mobile security has to change.

In 2011, tablet computers and smart phones will become a prime target for hackers/cyber criminals since they do follow the same rule of targeting the most popular platform used by the majority of the people.

Recommendations

- Treat your Android phone like unsecured PCs
- When downloading applications, make sure you're getting them from a trustworthy source – If you're unsure about the validity of an application, don't install it.
- Protect your Android smart phones with security software such as a AVG Mobile Security solution for Android's Smart Phones



About AVG Technologies

AVG Technologies is a global leader in security software, protecting more than 110 million consumers and small business computer users in 170 countries. Headquartered in Amsterdam, AVG is the fourth largest vendor of anti-virus software and employs close to 600 people worldwide with corporate offices in the US, the UK, the Netherlands, the Czech Republic, and Germany.

AVG has nearly two decades of experience in combating cyber crime and operates one of the world's most advanced laboratories for detecting, pre-empting and combating web-borne threats from around the globe for both businesses and home customers.

The company boasts one of the most extensive self-help communities on the Internet, having established its technology credentials early on amongst technically savvy consumers.

AVG has nearly 6,000 resellers, partners and distributors globally including Amazon.com, CNET, Cisco, Ingram Micro, Play.com, Wal-Mart, and Yahoo!