Pisco Med Publishing

Analysis of Network Security in Daily Life

Jinliang Shen,Shiming Gong,Wencong Bao

School of Computer Science and Technology, Shiyan University of Science and Technology, Hubei, China

Abstract: From the beginning of the new century to the rapid development of global information technology today, with the popularity of the Internet and the rapid construction of information technology, more and more people involved in the use of the Internet. Especially in the past two years, online surfi ng, e-commerce, online chat, e-government, Internet banking, online shopping transactions, online games, this series of network activities, has become a hot application of today's society. With the increasing reliance on the network and information technology in all aspects of society, the network has become an indispensable part of work and life for most people. The rapid development of the work brings closer the distance between real life and virtual world, changed the way people work, study and live. It can be sure that now the human life becomes more relaxed because of network. However, the network has brought us great convenience, but also brought some di ffi culties. Due to the design defects of the Internet itself and its complexity, openness and expanding of the software scale, the application is more and more complex, making the hidden danger of the network increased dramatically. Therefore, the security of the network has become one of the important factors hindering the process of information technology. Today, for many users, they know that they are facing a certain network threat. But from where, what will happen, are not very clear for many people. Generally speaking, ordinary network users mainly face Internet security issues. Computer viruses, cyber scams, data loss, botnets, phishing, privacy leaks, are a few example of network security threats. The recent impact of large events, such as: Panda burning incense virus, Trojan industry chain exposure, offi ce macro virus, Trojan horse site-linked malware, makes the network security issues become the focus of attention, even to worldwide audience.

***Keywords*:** network security; Internet; virus; information-based development

1. Network security

1.1. Definition of cybersecurity for daily life

If you must give the next definition of network security, network security is the information security on the network, and 'information security' have multiple understandings. All the deviation comes from the diff erent aspects of information security, so there have been 'computer security', 'network security', 'information content security'. There have been words associated as 'confi dential', 'authenticity' Integrity, " usability, 'and' non-repudiation, etc. '[1] The daily network security is of course the daily information security on the Internet.

1.2. Our network security around us

Nowadays, the development of the Internet to the homes can be a lot of aspects in life, a variety of entertainment, shopping, and o ffi ce works. Even government o ffi ce, military information, etc., can be carried out through the Internet. However, while network promotes competition, advantages will be taken by many of the ulterior lawless motives. Ordinary internet users enjoy the network for life, work, and learning convenience, but also in every moment are faced

doi: 10.18282/ics.v1i1.587

with a variety of network threats. Little carelessness will be costly.

1.3. Privacy disclosure

Our so-called privacy, that is, we do not want anyone to know some of our own secrets. But nowadays, personal privacy from time to time on the network will be exposed, and even some corporate secrets, state secrets are also stolen and published to the network, thus causing some potential sensational threat. Products we usually use such as network hard drive, Sina blog, internet banking accounts, QQ space, etc., if the operation password is too simple, or security questions easy to be cracked, will be capitalized by personnel with ulterior motives, resulting in personal privacy disclosure, loss of personal information, loss of personal property, etc. causing unimaginable consequences. It is advisable to carefully set passwords, you can set passwords with advanced relative security factor. It is to be remembered: do not set memorable account password such as birthdays, phone numbers and so on. Otherwise the loss will be immeasurable.

The commonly known 'Trojan' virus target the user account information, however in fact, as long as the security level to set a relatively high password, and removal of Trojan virus from the system, we can generally be able to more eff ectively deal with this threat. Trojan horse program is actually a computer virus, but its purpose is not to destroy the computer, but to steal your personal information, such as accounts, passwords and so on.

1.4. The biggest culprit in network security: computer viruses

Defi nition of computer viruses

The history of computer viruses can be traced back to the 1980s. If you want to give it a defi nition, it can be said that it is a set of computer instructions in the computer program to destroy the computer function or damage to the data, aff ecting the use of the computer and able to self-copy a set of computer instructions or program code. This is known as the computer virus [2]. It is destructive, reproducible and infectious. In the end, the virus is a computer program. It's every activity is not as revered as mysterious by ordinary people, a little understanding can defend us from most of the virus program.

Computer virus characteristics

Computer viruses do not come from sudden or contingent reasons. Occasionally a sudden power outage or occasional erroneous operation, some garbled characters or random commands will be disordered and chaotically generated in the computer's memory and disk. The virus on the other hand is a very strict, sophisticated, very orderly combination of a perfect code, and works with network system environment and adapt to each other to complete a certain instruction

main features:

1, Parasitic

Computer viruses, like parasites in the human body, are parasitic in the computer program. When someone executes the program, the virus will cause a damage to the computer. But before poisoning the program, it is not easily detected. Just as the same reason when people do not get sick, you will never fi nd the body's parasite.

2, Infectious

Infectivity is one of the basic characteristics of computer viruses. Computer viruses are not only very destructive, it has a very strong infectivity. The virus once the outbreak, copied or produce mutation, the speed is rapid and diffi cult to defend. It feels like a biochemical crisis in novels and fi lms. For example, the most contagious virus in 2007 is AV Terminator, while AV Terminator also creates strong destruction.

3, Latent

Hackers through timing, allow viruses works similarly as the timed bomb. Time of breaking out are pre-set. For example: Black Friday virus.

4, Hidden

Some viruses can be checked by anti-virus software for eff ective killing, and some are simply cannot be found out. Some viruses sometimes active and quiet and fi ckle. Dealing with this type of virus deal are generally very di ffi cult, as this is a very strong type of hidden virus.

5, Destructive

Sometimes a lot of Internet friends will find some of their own documents and information missing, or the computer will contain a lot of unknown documents, or click on an o ffi ce fi le will fi nd the contents of their own and the editor is not the same, or even garbled, or maybe that fi les on the D disk will be in E drive or desktop. It is likely that your computer suff ered a dev-

astating virus aggression. After the computer is attacked by such a virus, it will cause the normal program to run, and the fi les in the computer are damaged in varying degrees.

6, Can be triggered

The triggering of a computer virus refers to the occurrence of an infection or attack by a computer virus, such as: opening of the antivirus software, activates the outbreak of the 'AV Terminator'. Such similar features is called triggering.

1.5. Protection against network security threats

KeePass Password Safe tool

KeePass Password Safe tool is a password protection tool that can run on winME, win2000, winXP, WinVista, Win7, and other multiple operating systems. KeePass Password Safe is generated specifi cally for people who cannot remember a lot of passwords. It contains a powerful password generation engine and encryption storage function, providing a very secure password storage space. When we start using KeePass Password Safe, we fi rst decide a starting password. This password is used to identify people's identity, the password determines whether you can use KeePass Password Safe tool, so this password is absolutely not forgettable. After starting, you can store the password on KeePass Password Safe. In the KeePass Password Safe software, you already have some default password classifi cation. You can create your favorite password storage category as needed.

Note that KeePass Password Safe v2 Beta requires Microsoft .NET Framework ⩾ 2.0 or Mono ⩾ 2.0.1. [3]

Usage of security software

As shown in Figure 1-1, it is more difficult for ordinary network users to protect against network security, but if you use network security software for protection, all the operations are simple, for example, function of software such as 'computer physical examination', 'Trojan killing', 'loopholes repair', 'system repair', 'computer cleanup', 'optimize the acceleration' and so on are very perfect. So, I suggest that the majority of Internet users like you who do not understand much of computer network security protection, you can use the major free network protection software, which can be timely for your computer with a layer of protection, so as not to be more plagued with network threats.

2. Internet Banking Security

2.1. Definition of Internet Banking

排名	软件名称	月均月度覆盖人数（万人）2012.1-2012.6
1	360安全卫士	36935.3
2	360杀毒	36075.1
3	QQ电脑管家	8412.1
4	金山毒霸	8195.1
5	360保险箱	8084.2
6	瑞星杀毒软件	4632.4
7	金山卫士	4147.8
8	瑞星个人防火墙	1697.7
9	360系统急救箱	1002.6
10	金山网盾	974.1

注释：该榜单排名依据为2012年1月至2012年6月月均覆盖人数排名，艾瑞选取了月均覆盖人数大于100万的19个软件作为备选。

来源：iUserTracker，家庭办公版 2012.7，基于对40万名家庭及办公（不含公共上网地点）样本网络行为的长期监测数据获得。

©2012.8 iResearch Inc. www.iresearch.com.cn

Figure 1-1 China's Top Ten Antivirus Program in first-half of 2012

Nowadays, the way of online shopping is very diverse, one of which is online banking payment, many netizens which are new in online transactions often confuse network banking and payment platform, in fact, both have clear distinctions and connection.

Internet banking, also known as online banking, refers to the use of Internet technology, through the Internet to provide customers with account, sales, inquiries, reconciliation, inward transfer, cross-bank transfer, credit, network securities and investment/financial services and other traditional services, so that customers can safely and easily manage fi xed deposits, checks, credit cards personal investment etc. [4]. It can be said that online banking is a virtual bank counter on the Internet. Internet banking is also known as '3A Bank' because it is free from time and space, and can provide fi nancial services to customers at anytime, anywhere, in any way. [5]

2.2. Criminal use of network loopholes

Internet banking makes people's work and life is very convenient, making more and more Internet users use online banking for fi nancial management and payment. But the use of online banking in the process have many unsafe factors, seriously damaging the economic interests of Internet users. How cybercriminals steal Internet users account and password, cheat or steal money of friends and relatives of friends? Their main means of crime are listed as a few points:

1. Criminals issued a false bank website link to the netizens. They use a fake online banking website to send a link to the victim, and when the victim logs on to a fake online banking operation, he or she will be able to steal or modify the victim's account information.

2. Criminals use online phone and disguised as a bank staff . They impersonate the bank's customer service staff , to text and call to the victim, from there the victim's network account and password is retrieved.

3. Network hackers install the virus program on your computer to steal. They use the virus with a link, or the virus on a lot of unhealthy sites, when the victim clicks on site with the virus, the victim's computer will be infected with the virus, so as to steal the victim's online banking account information.

4. The perpetrators of Internet cafes or LAN management system eases the theft. Hackers installing Trojan virus in the Internet cafes or local area network server, so as to steal the victim's online banking information.

5. Set up false shops in the major shopping sites to fraud victims money. This kind of trick is to wait for users to pay the payment to the offi cial payment platform, and lure buyers to confi rm receipt after a variety of reasons. Once the buyer confi rmed receipt, the seller disappears.

2.3. Use of Internet banking must be guarded

How to prevent it, in view of these criminal means? I have also made the following few countermeasures:

1. During using online banking account, we must pay attention to identify the authenticity of online banking website.

During entering online banking, we should be carefully identifying whether the website is true or false. It is best to use their own collection of links or use Baidu, Sousou and other large integrated search engine to search online banking o ffi cial website. Figure 1.3.1-1 shows that usually the first site of the search engine will be the official website.

Figure 2-1 Baidu search engine search result of the ICBC online banking information

2. All the banks in the world will not send any information to customers for the account password, mail, and will not call customers to change the password etc. For bank staff to send text messages to customers or call customers, it will be done only through bank dedicated customer service phone. Even if you want to modify the relevant password, it is also only can be done on the o fficial website, or carrying the relevant documents to the bank counter for a similar business. Remember: as long as the caller ID or SMS display number is not the bank customer service number, then it must be false!

3. Remember in using the Internet banking, be sure to install the firewall software, genuine network antivirus software and security guards in the computer. It has to be updated in a timely manner and regularly killing the virus and Trojans. Do not view and unknown E- Mail, do not visit the unhealthy porn sites etc. to prevent a variety of computer viruses or hackers to invade your computer.

4. Remember to not in use the Internet e-banking in internet cafes, hotels and other public places, because public computer is easy to be infected by the virus attack or rigged. The usage of online banking in public is very dangerous, so users should avoid a similar situation as far as possible. Use personal computers at home for online banking related operations.

5. When browsing online shopping mall, we must wait until after receiving the goods to confi rm the quality of items is of no problem, the relevant accessories are in a complete set, before confi rming the receipt in the shopping platform. Remember, after confi rmation, account payment stored in the o ffi cial payment platform will be directly received by the seller.

Note: after the shipment by seller, the system is generally left to buy 10-15 days to confi rm reception. If the date expires, and you have not received the goods, remember to go to the site to cancel the transaction, or shopping site will automatically transfer your payment to the seller! [6]

3. The network security of mobile phones

3.1. The rise of mobile networks

In recent years, the upgrading of smart phones is extremely fast, high confi guration of phones basically has all the features on the computer. At the same time, the market price of smart phones and mobile networks, the rapid decline in network fees, resulting in the rapid formation of mobile networks. With this huge group of users more network threats are even more ubiquitous. So, when we enter the mobile network era at the same time, we must not ignore the network security.

Mobile networks are everywhere

Development of the mobile network today allows us to can pick up a smart phones with Android system installed for a few hundred dollars. Whether this phone is genuine or spin-off , when you activate the Internet network, you can enter anytime, anywhere into the network world to browse the web, online chat, microblogging, information search and so on. Most of these phones are even equipped with wi-fi function to connect directly through the wireless router Internet. As shown in Figure 3-1, is my Lenovo A798t search and connection to the wireless network signal. Of course, in addition to wireless network, we can also use the communications operators to provide the network for connecting to the Internet, for example: Mobile, China Unicom, and Telecommunications.

After connecting the network, you can either use built-in or download third-party software for Internet browsing. For example, my phone comes with a browser or QQ browser for web browsing, as shown in Figure 3-2, Figure 3-3.

Currently on the market of mobile phones, in addition to browsing the web, of course, there are many other network features, including specific features of the software and third-party software, such as mobile online video, weather forecasts, fl ight inquiries, QQ music, QQ chat Tools, 360 mobile phone antivirus software, etc. These wide variety of network applications have been widely available in smart phones. It can be said that the current market, most of the mobile phones are already a handheld computer.

Figure 3 Smartphone search for Wi-Fi signals Figure 3-2 lenovo A798t comes with a browser

Figure 3-3 through the wi-fi network to download the phone's QQ browser

3.2. Mobile phone network security risks exist

Now, smart phones as another terminal of the Internet, the same network security threats exist in mobile phones like in computers. For example, cell phone viruses, phishing and fraud information are some of the similar threats. As I mentioned in the previous chapter, for mobile phone there is a hidden risk on the fi nancial security. For example, the phone's stored call credit and storage information leakage.

At present the mobile phone or mobile Internet security problems are divided into four categories: mobile phone system security, mobile communication security, mobile (hardware) security and mobile privacy. Qihu 360's vice president, Tao Tao [7] thinks that mobile phone system security threats ranked fi rst, which one of the most commonly occurred is the mobile phone software malicious programs.

Savings of stored calls

Communication operator's communication services are required to have balance in mobile credit, that is, the credit balance of the phone must be available in excess, otherwise the communication signal will be disconnected. For example: China Mobile, China Unicom and so on. Of course, there are a small number of operators who are post-paid, such as Telecommunications. Phone credit are also linked to your other service, such as network broadband. Nonetheless, whether it is pre-paid or post-paid use, most cases mobile phone networks will be uesed, such as GPRS or the current market popular 3G work, but both their tariff s are relatively high. Especially

during beyond the usage of your allocated Internet quota, the cost is more than double.

A lot of malicious software capitalize on the mobile phone network traffi c vulnerability characteristics with frequent networking in the background, resulting in users to pay in high costs. Such as the famous SMS pirate Lanpackage, attacking the s60v3 system.

Lanpackage virus through the mobile browsing on malicious sites, automatically downloads the virus to the phone. After the virus is installed, the user's phone will be sending messages to random numbers, with the content: 'For all my private messages, please visit http: // ... ...', when the user received this MMS click on the URL, we can see the contents of the infected phone inbox, the recipient phone will also download the virus and automatically start. When the user receives the content, out of curiosity clicks on the 'view more' option, the virus will automatically download to the phone, hence starting a new round of infection. [8]

Mobile phone privacy

With the rapid rise of smart phones, mobile phone memory capacity also will increase sharply. In the current international market, the largest mobile phone memory capacity is 20GB, equivalent of a small capacity mobile hard disk. In addition to TF cards and external storage tools, it can reach nearly 100GB, equivalent to a computer. So more and more users will be storing important work or private information in the phone. Mobile phone use to this point, in addition to as a communication tool, it is moving towards a mobile o ffi ce assistant. Thus, the mobile phone stores a lot of personal privacy information.

3.3. Classification of mobile security threats

In fact, the main security threats to mobile phones, mainly comes from mobile phone malware and viruses. From its characteristics, mobile phone malware and virus threats can be divided into several categories:

1, Functional damage. Such malware and viruses are mainly based on the destruction of mobile phone systems and resource consumption, if your phone suddenly runs slowly, some programs cannot run or mobile phone features received restrictions, it is likely that it is infected by category of malware and viruses.

2, High cost of communication. This kind of malware makes you very frustrating, you find that your calls are plentiful, when checking your communication bill when you may find that you have opened a variety of special communication services, calling a Japanese star or a foreign senior leader called. Do not be surprised, your cell phone is clearly invaded by mobile phone virus. These malware goes using your number, and then send text messages to inform the communications company to order a variety of high-cost network services, so as to achieve the purpose of consuming your telephone charges. Agency analysis shows that such malicious virus cost Chinese mobile phone users up to millions of losses daily.

3, Information theft. This is the same principle in malicious software, assuming you accidentally installed this type of program, or because the mobile phone system by virus attack, then there is no doubt that your photos, SMS, call records, and even payment accounts are in the risk of being leaked.

4, Destroy of reputation. If your cell phone is infected with this kind of malicious virus software, then, congratulations, you will be famous among your phone contacts and QQ contacts. Of course, this is falling into bad reputation!

The above four categories are currently the most typical mobile phone security threats, their main purpose is to obtain economic benefi ts, and even worse may be just a boring funny software or virus. With the continuous upgrading of mobile phone technology and the evolution of virus Trojans, a variety of malicious software threats will certainly be endless and increasingly updated, making many users of mobile phones frightened.

3.4. Prevention of mobile security threats

The previous section already mentioned that after the phone is infected with a lot of viruses, the private content inside will be in a serious threat. There are some threats, it is directly related to privacy data security, including mobile phone theft and so on. In large crowds of shopping malls, stations, pedestrian street and other places, frequent theft of mobile phones occur. People at the same time in losing mobile phones bear the risk of disclosure of private information and important information.

For the above mentioned mobile phone security threats, I put forward some suggestions to protect the privacy of mobile phone users and privacy.

Custom fl ow packages to save costs

In order to prevent malicious software using mobile phone traffi c to generated high cost, I suggest that the majority of users, according to their actual situation to customize a suitable mobile data package. Here I am usingthe largest mobile communications service operator in China, China Mobile as an example. For example, Hangzhou Mobile data packages as shown in Figure 3-4.

From the fi gure we can see, package in Hangzhou is the most expensive about 6Mb / yuan, that is, 1 penny gets 0.06Mb, 61.44KB, which is equivalent to browsing a picture. Without the data package the price is outrageous, equivalent to 10 yuan / Mb. It can be seen, subscribing to appropriate package according to our own traffi c, in fact, is an eff ective way to prevent the invisible loss of credit.

And, as far as I know, Hangzhou and a small number of domestic areas have begun to popularize China Mobile's 'mobile internet partner' 4G Internet packages, the minimum monthly subscription of 30 yuan / month for access to 2G of Internet traffi c. It is the gospel for mobile phone lovers.

Use mobile phone anti-virus software to prevent the virus

Currently on the market a lot of software providers, have launched a mobile version of the security software against malicious software, such as Tencent mobile phone housekeeper, Baidu security steward, Jinshan mobile phone drug tyrants, 360 security guards and so on. This article uses Tencent mobile phone housekeeper as an example, showing the mobile security software interface. This is shown in Figure 3-5.

Representation of the operator to the unknown fee

Currently there are many malicious software on the market itself is a wolf wearing a sheepskin, on the surface it shows a free game, or have certain functions, but when function is running, it will immediately deduct a lot of users value-added services. This is basically daylight robbery, the user is often directly bear serious consequences. Most of this is because of inadequacy of Chinese networking law and regulations.

But if the user encountered a similar situation, then I suggest, it is better to try to call the communication operator's customer service. If the malware can be frozen, then the deducted costs are likely to be recovered, even if the loss is not recovered, this can also a mean to expose malicious virus software under the sun, so as to remind more mobile phone users to be careful under these threats.

1) mobile phone housekeeper user interface 2) mobile phone housekeeper virus security control interface

Figure 3-5 Tencent mobile phone steward interface display

References

1. Wang Shujiang, ed. Super network management must learns: network security. Beijing Machinery Industry Press, 2007-9, ISBN: 978-7-111-22273-6
2. Wang Peichang, ed. Computer virus secret and confrontation. Electronic Industry Press, 2011-10-1, ISBN: 978-7-121-14605-3
3. Liu Baoxu, Jiang Wenbao. Wang Xiaizhen, ed. Active defense on hacking. Beijing Electronic Industry Press, 2007-11 ISBN: 978- 7-121-05103-6
4. Wang Shan, Li Guangpeng, Shi Yanyan, ed. Internet age life security strategies. Mechanical Industry Press. 2011-1, ISBN:978- 7-111-32420-1
5. Shuai Qinghong, ed. Institutions of higher learning e-commerce professional planning teaching materials: online payment and online banking. Mechanical Industry Press. 2010-4-1, ISBN: 978-7-111-30379-4
6. Du Weifeng, Liu Wenting, Wang Dada, ed. Enjoying electronic payments: A complete guide. China Railway Publishing House. 2012-2-1, ISBN: 978-7-113-13875-2
7. Wang Jigang, ed. Mobile phone virus exposure. Xi'an Jiaotong University Press. 2009-10, ISBN: 978-7-560-53220-2
8. Wang Jigang, ed. Mobile phone virus exposure. Xi'an Jiaotong University Press. 2009-10, ISBN: 978-7-560-53220-2