SILVER SURFERS’ ON-LINE SAFETY GUIDE
BASIC TIPS ON SAFE COMPUTER AND INTERNET-BASED ACTIVITIES

SABINA DATCU, IOANA JELEA
E-THREATS ANALYSIS AND COMMUNICATION SPECIALISTS

FAMILY, SENIOR USERS
Table of Contents

Table of Contents ...............................................................................................................................2
Are senior citizens considered a target by cybercriminals? ............................................................4
Finding out what you’re dealing with on the Internet .................................................................6
Q1: What is malware? .....................................................................................................................6
Q2: What is phishing? ......................................................................................................................6
Q3: What is spam? ..........................................................................................................................7
Q4: What is spyware? ....................................................................................................................7
Q5: What is adware? ........................................................................................................................7
Q6: What is a virus? ........................................................................................................................7
Q7: What is a Trojan? ......................................................................................................................8
Q8: What is a rogue antivirus? .....................................................................................................8
Q9: What is a keylogger? .............................................................................................................9
Case studies .................................................................................................................................. 10
Seniors as main target ....................................................................................................................10
  Pension delivery spam ..............................................................................................................10
  Fallacious tax-paying methods ...............................................................................................10
  Income-related spam ..............................................................................................................11
Seniors as secondary targets ........................................................................................................12
  AOL phishing attack .............................................................................................................12
  Rogue distribution ..................................................................................................................13
  Malware spreading via e-mail ...............................................................................................14
Senior net surfers’ golden security rules ....................................................................................15
When browsing the net..................................................................................................................... 15
Computer protection.......................................................................................................................... 15
Browser version and surfing security................................................................................................. 16
Personal data protection...................................................................................................................... 17
When using the e-mail.......................................................................................................................... 17
Avoiding unwanted e-mail.................................................................................................................. 17
When using instant messaging applications..................................................................................... 17
When making online payments........................................................................................................... 18
Do not be afraid to report..................................................................................................................... 18
Choosing a data security solution........................................................................................................ 20
Is there a language barrier?................................................................................................................. 20
Does the solution cover all my needs?.................................................................................................. 21
How much of my input will be required?............................................................................................. 22
Can I get help?...................................................................................................................................... 23
Are senior citizens considered a target by cybercriminals?

At a first glance, it would appear that senior citizens are exposed to cybercrime just as much as any other inexperienced Internet user, irrespective of their age. Still as a general rule, in order for their malicious schemes to succeed, cybercriminals tend to appeal to common elements of the human psychology: curiosity, greed, empathy.

Why do senior net surfers get this “special treatment”? According to a set of fraud prevention guidelines published on the FBI website, entitled Fraud Target: Senior Citizens, experience has shown that senior citizens are preferred cybercrime targets due to a combination of psychological, economic and social factors specific to this age group. Here is a summary of these factors:

1) Senior citizens are generally targeted because they are more likely to have money, whether as life-long savings, property or as investments.

2) Due to the way they were educated, senior citizens tend to be more trusting and less aware of the evolution of scam techniques. Add the likelihood of their being alone (because they have busy families or no family at all), and you’ve got one other very important ingredient to this mix: they probably do not have anyone to ask for guidance. Plus, depending on their previous experience, they might be vulnerable to situations in which they are approached by “benevolent” strangers or, exactly the opposite, quite skeptical about this kind of scenarios.
3) Assuming that they have only recently been introduced to computers and the Internet, senior citizens, just like any other beginners in this domain, are probably less likely to realize that they have been victims of cybercrime right away. The time gap between the event proper and the moment the crime is reported might pose some problems with respect to how accurately the victims remember the details of their online activities.

4) Hope in the evolution of medical science combined with the need to cope with various age-specific conditions makes the promise of new medical products, cures and vaccines very alluring for senior citizens. An equally valid motivation in this respect is the promise of discounted prices.

Another element to be considered here, but which is not age-specific, is that people are generally disinclined to report any online incident they were a victim of, either out of shame or because they would not know what state or police authority to turn to. This hinders the scam tracking process, it reduces the reaction speed of authorities and it puts victims through lengthier recovery processes.

Hence, there is some degree of vulnerability that is specific to the category of senior Internet users, but it is also true that in most other respects, all Internet users are equally exposed to e-threats if not properly informed about them. As computer literacy becomes a requirement in education systems, this problem is likely to become less severe across all age categories. Practically, if all people who have access to the education system acquire basic computer knowledge, their skills in this domain will not be connected to their age anymore.
Finding out what you’re dealing with on the Internet

The most important piece of advice would be for you to get familiar with what the Internet can do and with the applications you are supposed to use online (browsers, chat, online payment, etc.). Try to find a reliable source of information on what potentially dangerous actions can be performed using each of these applications. Don’t be afraid to ask “What happens if I do this?” as any click is important when it comes to your security on the net. You can find plenty of information about these topics and others on the BitDefender website and on the BitDefender security blog.

After all, knowing what risks you are taking when engaging in a specific online activity will make you less prone to falling into cybercriminals’ traps. Here are a few security-related questions and answers you might start from before using the Internet:

**Q1: What is malware?**

This term designates any kind of computer program created with a malicious intent and which aims to tamper with the operation of your computer, render your stored information unusable, steal your personal data for financial gain, etc.

**Q2: What is phishing?**

This is the name given to a mechanism cybercriminals put together in order to trick people into giving them personal data (e.g. credit card numbers, PIN numbers included). To get this information, they create lookalikes of trusted web pages (banks, social media applications, state authorities, etc.). Mistakenly believing that they are dealing with the real thing, users will type their data and expose themselves to the risk of financial loss.
Q3: What is spam?

Spam is the name given to the unsolicited e-mails sent to large groups of people, generally to advertise various products. These e-mails are also used as baits in more complicated malicious activities, such as phishing.

Q4: What is spyware?

These are programs that install on your computers, without your knowledge, the equivalent of a stranger’s eyes peering over your shoulder to see what you are doing, what you need and what you are looking for. Usually, the curious stranger is a hacker or another type of cybercriminal.

Q5: What is adware?

These are programs that allow pop-up windows to appear on your screen and to display advertisements about products they might be interested in. How do these programs get information about your preferences? This is where spyware comes in handy.

Q6: What is a virus?

A malicious program that is intended to disrupt your activities on the computer by damaging your operating system and by corrupting or making inaccessible the information stored in your system. Different from other forms of malware, a virus is capable of copying itself, therefore infecting the whole computer. By attaching itself to a host, which can be carried to another computer (e.g. on a CD, a DVD or a USB drive), the virus can easily spread to other computers as well.
Q7: What is a Trojan?

Just as its name suggests it, this is an apparently inoffensive computer program which actually allows a hacker to gain access to your system. Once installed, the Trojan serves as a means for the hacker to steal your data, install other malware, and, generally, to monitor and interfere with your computer activity.

Even after this initial familiarization stage, don’t be afraid to ask questions if you are not sure what to do online or what consequences your actions might have. This is to say that an ongoing process of learning how to act cautiously on the web is preferable to just refusing to access a whole world of online resources because of the underlying sources of danger. This might seem a lot to deal with, but once you have installed and use a reliable security solution, most security problems will be taken care without any effort on your side.

Q8: What is a rogue antivirus?

This is malicious program that tries to persuade you to download it by disguising itself as an antivirus. First, several pop-up windows alert you about a series of security problems detected in the system. These problems are not real, but they are intended to create panic. If you accept to download what they present you to be an antivirus that will solve these problems, you will get your computer infected. This includes being spied on in all sorts of ways, which may culminate with cybercriminals taking complete control over your system.
Q9: What is a keylogger?

A keylogger will monitor your activity by tracking the keys you strike on your keyboard. These applications may come with added features such as the ability to transmit the results of the monitoring activity over the Internet, to take screenshots of your screen, etc. Some keyloggers can even track passwords that appear on the screen as hidden behind asterisk masks.
Case studies

The e-threats created with senior users in mind can be divided in two major classes: directly and indirectly targeted. Here are a few case studies illustrating the behavior and consequences of each category.

Seniors as main target

Directly targeted malware spreading mechanisms greatly rely on the use of spam messages related to errors in pension delivery, fallacious tax reduction methods - almost always accompanied by malware - and, sometimes, fake job offers dedicated to retired persons.

Pension delivery spam

This first example presents a spam e-mail related to a supposed error in pension delivery. To persuade the recipient of its legitimacy, the message uses an official language. Nevertheless, its only purpose is to steal sensitive information such as users’ name, address, phone number, occupation.

Fallacious tax-paying methods

The second example refers to fallacious tax-paying methods. Using attractive photos of happy seniors living their lives as a background, these sites manipulate their visitors into revealing personal data, including their name, address or bank accounts. With these key elements on hand, the only thing left for cybercriminals to do is to leisurely drain the money from the accounts to which they gained illegal access.
Income-related spam

The third case study presents an unsolicited message which requires the recipients to review their underreported income statement. This message, identical to the one previously used to deceive IRS recipients, is employed as bait in a personal data harvesting scheme.

The alleged customized link does not lead to Her Majesty’s Revenue & Customs’ Web site, but to a Web page which mimics a personalized download location, employing several visual identification elements of the original site, such as the logo, header or formatting elements.

The page also provides a link to a purported tax statement that the user should download and execute. Despite the appearance of legitimacy, upon clicking the link, the user does not receive an e-form, but a cocktail of malicious payloads, as illustrated in the image here to the left.
Seniors as secondary targets

The e-threats indirectly targeting seniors are represented by rogue antivirus software, phishing attacks or malware-infected websites. Their indirect approach practically means that they are not specifically designed with this user category in mind, but that they have an all encompassing scope. They will be considered in this guide because they are important malware sources and senior citizens should be aware of them.

AOL phishing attack

AOL members find in their inboxes an apparently legitimate message whereby they are asked to update their personal data. The ensuing phishing mechanism is simple and it aims more targets in one go: AOL users’ account records, personal – sensitive data and other information required for “password recovery”, in general.

The fake official AOL e-mail places users under pressure to provide the required data by setting a clear deadline– January 31- and by specifying that if they fail to do so, their accounts will be suspended.

The e-mail also includes a special link that users must click in order to confirm their AOL e-mail account and password. The link leads to a fallacious AOL webpage, carefully crafted to deceive credulous users.

And the phisher gets greedier: the next step takes AOL users to a page where they are supposed to fill in various personal information, such as: name, address, credit card number, social security number.

In this final step, a request for an apparently trivial piece of information slips in: mother’s maiden name. Considering that this detail serves as a password recovery hint for e-mail addresses or online banking accounts, this last move should make the alarm bell ring quite loudly.
Rogue distribution

Cybercriminals continue to rely on their victims’ curiosity in order to trick them into imperiling their data. In the “Internet hot topics” scheme, the malware spreading mechanism is simple and classic: when the credulous user clicks the link to an apparently legitimate Web site displayed in the search results page, the browser is automatically redirected to a Web page that infects the computer with a fake antivirus.

The behavior of the malicious program starring in this case is comparable to that of other rogue antiviruses: when the user is redirected to the malware distribution Web page, the browser window automatically minimizes and a warning message simultaneously displays. This message notifies the user about several alleged computer infections and it points out the necessity of installing a security solution.

By clicking either the OK or the Cancel buttons of the various pop-up windows appearing on the screen, the user activates a false demonstration that unfolds in the restored browser window. This demonstration imitates an on-going scanning process that detects oodles of malware in the system, while other fake pop-up windows attempt to trick the user into downloading the malicious program posing as the antivirus.

With each so-called scan, more and more notices of false detections place the user under the pressure of registering the rogue antivirus. Once installed, it modifies or irretrievably damages the content of several system files and it conveys numerous pop-ups on sham system problems and fake infections, while also persistently asking the user to buy or renew a license.
Malware spreading via e-mail

There is one category of spam which fraudulently uses very well known brands in order to spread malware. Here is an example of such a situation:

An unsolicited e-mail states that a well known shipping company has a problem in delivering a parcel, because the postal address is wrong. In this case, the recipient of the notification is guided to print an address label, attached to the mail as a .zip file and, using it, to pick up his or her parcel from the post office.

However, the message is not from the real company and the claim that the parcel delivery failed due to an address error is untrue. There is no parcel, the message being just a trick designed to fool recipients into downloading the attachment. If they do that, instead of an address label, the users receive malware.

Once installed onto the system, this malware might try to download and install other e-threats, such as keyloggers, password stealers and rogue antivirus software.

The social engineering techniques behind this malware distribution campaign prove to be efficient. Whether they use the real company’s services and are expecting a package, they think that somebody sent them a gift, or they are just curious to see the details within the attachment, the recipients of this e-mail are very likely to fall into the trap. In all cases, the result is the same: open the file to take a look inside and ultimately… get infected.
Senior net surfers’ golden security rules

Stick to a few common sense online security rules. In other words, do not take more risks online than you would in your real life everyday activities. Just as you choose to lock your doors at night and not to share your bank account number with any stranger on the street, do not allow unknown citizens of the cyber world to access your computer or your personal data.

Here is a set of preventive measures that will help you stay on the safe side of online experiences.

**When browsing the net**

**Computer protection**

The first thing to do is to install, activate and constantly update a reliable antimalware solution, capable of protecting you against a wide range of e-threats (viruses, phishing, spam, etc.). BitDefender data security solutions, for instance, will secure all of your online activities. This means that you will be warned whenever you get into a situation that might be dangerous for you, such as accessing a forged site. Also, the security suite will block any virus as well as other e-threats before they can damage your computer and data. Installing and activating such a solution is a matter of minutes, while the updating process is automatic.

Once you have completed this first step, you’re ready to explore the web.
Another simple, but efficient piece of advice is to make sure that you are using the latest version of your Internet browser (Microsoft® Internet Explorer, Mozilla Firefox, etc.). In this way, you will not be bothered with unwanted advertising windows (pop-ups). Browser version updates are automatic, in most cases. However, if you want to find out what version you are using or how to update it, either access the Help menu, About section of your browser or open the browser and press the F1 key.

When you open certain web pages, small windows might pop up and try to persuade you to click them under various pretexts: winning something, trying a new game, accessing another web page. In most cases, your browser will block these windows, as this feature is enabled automatically.

However, if you encounter pop-ups while surfing the net, avoid clicking the links they contain, as you never know what hides behind them.

Do not install software on your computer without first consulting with a specialist, for instance the sales consultant at your local computer store, or a relative with knowledge in the domain.

Beware of pop-up windows which invite you to download software in order to get protection against an alleged security problem.

If you click the link provided you will probably end up on a web page that looks perfectly normal, although it actually represents a door for malware to be downloaded to your computer.
Personal data protection

Do not enter your e-mail address or other personal information on suspicious web sites. Similarly, avoid listing your e-mail address in guest books, on forums, etc. This will help you avoid getting your Inbox flooded with spam messages and stay protected against identity theft (situations when your personal data is used to impersonate you for financial gain).

When using the e-mail

Avoiding unwanted e-mail

A good idea would be to have two e-mail addresses: one for correspondence with the people you know, the other to be used when you are required to enter your e-mail address in order to access an Internet service. This separation will help you manage the problem of spam, for instance, as your personal e-mail Inbox will not be clogged with unsolicited commercial messages.

Do not open e-mails or attachments from unknown senders or with suspicious/ unusual subject lines.

When using instant messaging applications

Do not click any link you receive via your instant messaging application unless you know one of your contacts actually sent it to you and made sure it’s safe.

Messages containing links can actually be generated automatically, by a malicious program, which uses the names on your list of contacts to trick you into clicking and getting infected. That is why simply asking that person whether he/she actually sent the message will keep you safe.
Similarly, make sure the files you receive through your online chat application are safe and scan them before opening them.

**When making online payments**

Think carefully before responding to any investment offer that seems to be exaggeratedly advantageous and requiring that you act “right now, before it is too late”. Similarly, do not respond to offers/inquiries that you do not understand.

Before making online payments, you should make sure the page you are on is secure. How can you tell that the page is secure? Secure web pages use a data encryption system called **Secure Sockets Layer (SSL)** so that your sensitive information is made unusable by anyone who may want to steal it while it travels from your computer to the bank’s server.

There are two visible signs that the web page is secure: its address starts with **https://**, where the letter “s” stands for secure, and there is a lock icon in the internet browser.

When clicked, the icon should display information about the security of the site.

Considering that this security check is a matter requiring some degree of technical knowledge, if you have any doubts about it, please consult a specialist before making any payments (for instance your financial advisor).

Avoid using a non-secured computer or a public computer connected to the Internet (such as in a café, at a library). Make sure that you know and trust the owner of the access point; also, refrain from using an unsecured public wireless connection (like those in airports or hotels) when sending data over the Internet.

Discuss your financial affairs only with your family, trusted friends or your personal bank employees.
Ask for tenders and bills exclusively in writing and do not make advance on-line payment for goods or services.

Do not disclose your PIN to anyone, under any circumstances. In phishing attacks, cybercriminals will create fake web pages of trusted institutions that provide online payment services or which require the creation of an account in order to gather the victim’s personal data, among which PIN numbers, which are never to be disclosed.

Do not be afraid to report

Reporting fraudulent or malicious activities will very likely prevent the propagation of the phenomenon and it will help those affected recover or limit their losses. Stepping forward and requesting the support of the authorities is crucial.

If you think you have been tricked into giving money to online scammers, you should immediately inform your bank or credit card company to have your account or credit card blocked. You can also ask for help at your nearest police station and call the local consumer protection authority to find out how you can deal with Internet crooks.
Choosing a data security solution

A reliable data security solution will help you avoid online booby-traps. The main issues at stake when making this choice are the following: how efficiently the solution identifies and blocks e-threats and how easy it is for you to use it.

As far as efficiency is concerned, opting for one antimalware solution over the others is based on a combination of elements, such as the speed with which it reacts to new threats, how high its detection rate is, whether it has the capacity to act proactively (i.e. identify and block threats before they are officially “signed”), etc. BitDefender offers a complete suite of antivirus solutions adapted to various usage scenarios.

On the ease of use side, it’s mostly up to you to decide what best suits you. Here are a few practical things that you might take into account:

**Is there a language barrier?**

Make sure the data security solution is available in your local language so that you will not find yourself at a loss in front of cryptic pop-up messages. The BitDefender solutions, for instance, are available in 18 languages. For more details on your localized version, please consult the BitDefender website.
Safeguard Your Privacy

Eliminate the chances your data and conversations are leaked to others over email, Facebook, IM, or websites that track your online activities.

Stop Viruses and Spyware Cold

Proactive protection stops new viruses and malware that other products miss.

Choose Your View

Match the interface to your level of comfort by selecting between Basic, Intermediate, or Expert settings—and quickly create shortcuts to frequently-used controls.

Does the solution cover all my needs?

Compare the list of activities the solution promises to protect to your own online needs and get familiarized with the kind of warnings it will issue in dangerous situations (if any).

The example below represents the BitDefender antiphishing warning screen. This means that when you are about to enter a web page that has been identified as being set up to steal personal data, you will be warned of the risk you are taking.

```
BitDefender Total Security 2011

This webpage may be potentially unsafe and has been blocked by the BitDefender Antiphishing Module.

If you think the page is safe, please click here to add it to the whitelist so that it will not be detected as phished again.
If you want to see the webpage only this time, click here.

WARNING: providing personal details on this page might not be safe.
```

Fig. 20 BitDefender leaflets help you make an informed choice

Fig. 21 BitDefender Antiphishing warning
How much of my input will be required?

If you choose one of the BitDefender solutions, it will be up to you to decide how much you want to be involved in the way that solution functions.

As illustrated in the example here to the left, you can decide how much of the product you want to customize while running the initial configuration wizard. With just one click, you can opt for an easy or for a custom setup.

You can also decide how many details you want to know about the data security activities on your computer. By choosing one of the three available product views - Basic, Intermediate, Expert - you can interact with the solution as much as you like, or even just let it run in the background and only focus on your other computer activities.
Can I get help?

It is important to know where to look for answers when you need them. The solution’s user manual comes in handy, especially if it contains clear, to the point instructions.

For instance, if you want to get more details on how the BitDefender solutions deal with the issue of spam, you can consult the corresponding section of the manual. This is where you will find out: that spam messages are marked with [spam] in the subject line, what mail clients the solutions work with, where to find the identified spam messages, depending on the mail client you are using, etc.

In addition to that, support is readily available in case you need it. All BitDefender solutions provide Smart tips: precise and personalized explanations on how to use your computer safely and under best performance conditions. Moreover, by confirming your e-mail address, you can make sure that your e-mail support requests reach the BitDefender Customer Care team and that they are dealt with quickly.
The information and data ascertained in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender’s commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible postrelease information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publisher, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2010 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.