2
Where to Go for Assistance

Help Available

Being secure in your use of the Internet in today's world is difficult, but there are a number of services out there that can help. In the last few years the range of electronic services available to consumers has mushroomed, and this is a great boon in many ways. Many goods and services are available at lower costs, and the range of options has increased. Unfortunately, expanded opportunities available via the Net come at a hidden cost. That cost is exposure to cybercrime and unwanted spam messages. If you have children there is also the risk of them being exposed to pornography or inappropriate information.

In the world of the Middle Ages, information was a scarcity. There were very few books, and they were all handcrafted. The cost of a single book was huge, and only the elite could access most of the world's knowledge. Over the centuries information has become more and more accessible, and the cost of obtaining information has plummeted. It was said in the 1980s by Richard Solomon of the MIT Media Labs: "Someday in the not too distant future we may be paying more to screen out unwanted information than we pay to get the information we want."

In a world of increasing information overload Richard Solomon's prediction seems to have been incredibly insightful. Indeed we have increasingly been forced to purchase anti-virus filters and firewalls to screen out malware and install spam filters to free ourselves of unwanted solicitations. If one looks at today's world of information retrieval in this context, then the equation becomes clear. We are paying less for most of the information that we receive, and the corollary is that we are now paying for what can be generally characterized as cybersecurity. Thus the still-modest costs of filters

J.N. Pelton, I.B. Singh, *Digital Defense*, DOI 10.1007/978-3-319-19953-5_2

and protective services to keep out unwanted information is just the cost of getting information in today's world.

Today's millennials—let's say people under 30—in general don't subscribe to newspapers or listen to the 7 or 11 o'clock news but simply get their news online. They can purchase much of what they want or need online. The cost of electronic filters to protect against cybercrime and identity theft is on balance less than a newspaper subscription. The devil's bargain is that if you want cheap information off the Internet you have to pay for it by buying some form of cybersecurity and getting professional assistance to help protect against identity theft, ransomware extortion, or other forms of electronic intrusions into your life.

Oddly enough, the easier job that you might undertake to protect you and your family might be in buying and installing various forms of cyber protection that you can buy online, such as we will describe to you in the following pages. For an amount of about $60–$75 a year, if you invest wisely, you can buy cyber protection that includes antivirus, a good firewall, identity theft protection and insurance. You can also learn a number of things to look out for that might lure you into a cyber-correspondence that might lead to theft of your assets or problems with your computer. The number of phishing and pharming scams out there is only going up despite more cybersecurity enforcement. This is in large part due to the fact that black hat hackers come from many countries where enforcement policies are lax.

The bigger challenge may come in trying to protect you and your family against cyberbullying by so-called cyber "trolls" that stir up mischief or worse. Along with these cyber-attacks against your family, and particularly teens and tweens, there are problems associated with pornography on the Net and the temptation of so-called "sexting" (i.e., sending nude or compromising pictures of oneself or others over the Internet). Further there are a lot of hate e-mails out there that come in the form of racial, religious or sexual orientation bigotry or terrorist-generated messages that can be hateful to members of your family or could provide the wrong type of influence on your family and loved one.

The first part of Chap. 2 outlines various services that are available to you to protect you against cyber-criminal attacks that could disable your computer, lead to substantial financial losses, or other nefarious results. These are the most straightforward safeguards we advise you to use. These are forms of protection that can help you defend your computer, cell phone, and other electronic devices against cyber-attacks. Later in Chap. 5 we return to address security for cell phone and instant payment programs such

as "Apple Pay." Also in Chap. 2 we discuss some of the services that are available to address and assist with the problem of cyberbullying and cyberbullying alert services.

The last half of Chap. 2 shifts from a discussion of security measures such as anti-viruses and firewalls, to the problem of unwanted content and messages that can make the lives of you and your loved ones miserable. Here, as we noted in earlier, comes the hard part. This is because we are trying to block, mitigate or stop unwanted and unkind content from flowing to you and your family and stopping trolls from polluting the Internet with untrue and hurtful messages about your loved ones. This is difficult and challenging to deal with but also an area where protective actions are possible and the most vicious and harmful "trolls" can be shut down.

First let's protect your computer against cyber-attacks. We have already outlined some of the common sense steps you should take to protect yourself and your records. Now let's examine the type of assistance you might wish to obtain.

Electronic Filters That Protect Against Malware Intrusions

The first thing you should do is have a good Internet antivirus software package. Here, for instance, is what Norton Management, among others, claims to provide. We provide this list because it is a comprehensive statement and is typical of what a antivirus service should provide. We would like to emphasize that in this book that seeks to provide objective advice, the specific examples provided in this chapter or elsewhere about service provider offerings is not an endorsement of these products. We suggest you go to the consumer rating sites to make your individual choices [1] (Table 2.1).

For about $60–$75 per year or less one can purchase and install one of the top cybersecurity software packages offered by McAfee (now owned by Intel Security), Kaspersky, Bull Guard, ESET, Norton (owned by Sematec), or any of the other options listed on below. The higher prices can include protection for multiple devices (Norton covers up to five or even ten devices for instance at an additional charge) as well as security backup protection. This backup protection is actually quite important and useful. If you have a number of important documents and photographs that you consider vital, it is important to have automatic backup of this information against a cyber-attack. Norton service claims in Table 2.1 are used only as an example and not as a product endorsement.

Table 2.1 What Norton claims its software products can do

Key features
Actively Protects Against Viruses, Spam, Identity Theft, and Social Media Dangers
• Insight identifies which files and applications are safe and which are dangerous, using the combined feedback of more than 175 million Norton users.
• Norton Community Watch tracks virtually every file on the Internet for comprehensive global threat monitoring.
• SONAR Behavioral Protection detects signs that a file is dangerous to proactively protect you from never-before-seen threats.
• Spam blocking keeps your mailbox free of unwanted, dangerous, and fraudulent emails.
• Internet Protection System scours websites and social networking sites for suspicious links and content to identify the latest social networking scams.
• Download Insight and IP Address Insight to prevent you from downloading files from websites that have a low reputation score within the Norton user community.
• Live 24 x 7 Threat Monitoring is backed by a network of Norton users who serve as your own personal Neighborhood Watch group.
• Scam Insight reviews a website's reputation and lets you know if it's safe to enter your personal information.
• Anti-phishing technology blocks fraudulent "phishing" sites set up to steal your personal information.
• Identity Safe remembers, secures, and automatically enters your usernames and passwords for you, so they can't be lost or stolen.
• Parental control feature helps you protect your children from online dangers by giving you direct access to Norton Online Family.
• Safe Web tells you if a website is unsafe before you visit it, and it's too late.
• Safe Web for Facebook scans your Facebook wall and news feed for URLs containing security threats such as phishing sites, malicious downloads, and links to unsafe external sites.
• Intelligent 2-way Firewall prevents strangers from accessing your home network by blocking incoming traffic determined to be unsafe.
• Network mapping and monitoring shows all the devices connected to your home network, so you can spot uninvited guests using your wireless connection and/or eavesdropping on you.
• Automatic silent updates keep you one step ahead.
• Automatically downloading of updated products and installing important product and feature updates when you're not using your computer.
• Norton Pulse updates virus definitions every 5–15 min without disrupting work or play.
• Insight + Optimized File Copy identifies safe files and only scans unknown files.
• Built-in Intelligence maximizes battery life by putting off non-critical activities until you are plugged in and out of full-screen mode. (Table provided by Norton -by Sematec)
• Norton Management enables easy single-password access to all Norton Cloud-based applications and web properties

Matchtop's Top Ten Antivirus Sites evaluation (see below) of what it considers the best programs out there, based on levels of protection and cost, uses a 5.0 scale, with 5 being the highest rating [2] (Table 2.2).

Table 2.2 One assessment of various antivirus software commercially available

Rating the top ten antivirus sites for performance and cost[a]		
Company	Rating[a]	Cost/year
McAfee by Intel Security	4.9	$24.95
KasperSky	4.5	$29.95
Bull Guard	4.5	$23.95
ESET	4.5	$20.15
Norton by Sematech	4.4	$35.99 (for up to five devices)
Trend	4.4	$29.95
AVG by Microsoft	4.4	$31.99
Zone Alarm	4.3	$44.95
VIPRE	4.2	$39.95
PANDA	4.1	$39.95

[a]See the website address given below for details about the ratings

It is recommended that you explore all of the three sites indicated below. These websites provide a very useful assessment of various antivirus materials that are currently on offer. Some are better at providing instant updates. Others offer better protection against phishing or certain types of malware. The main thing in making your decision is that there are number of websites that can provide useful advice. In addition to the three websites provided below, Consumer Reports and the AARP websites are also quite helpful. One of the major things that should be considered in making your choice of a cybersecurity package is how many devices do you wish to protect? If you protect your home computer but not your smart phone or laptop or netbook or your IPad, Kindle, Nook or tablet, you could be in for big trouble. The issue of mobile services and cybersecurity we address in Chap. 5.

Recommended Websites

http://antivirus.thetop10sites.com/
http://www.top10antivirussoftware.com/
http://www.pcmag.com/article2/0,2817,2388652,00.asp

It should be recognized that the above list of ten is still not comprehensive, and that there are other products out there such as “Avast”, “Aviro”, “BitDefender” and “Pareto” plus others that should be seriously considered. This is particularly the case with Avast and Avira because their basic level of

protection is for free. If you are going to focus on just free services, we suggest that you go to the *PC Magazine* site (http://www.pcmag.com/article2/0,2817,2388652,00.asp) that does an independent evaluation.

Indeed there are several cybersecurity products out there that allow "free" antivirus downloads. These include offerings from organizations such as Avast.com or Avira.com. These organizations provide free downloadable antiviruses, at least for their lowest level of protection—and sometimes the antivirus is only free for just a year. Of course, higher levels of protection are available for a fee. These groups' marketing strategy is to offer free service as an entry point to sell their additional software. Also, if you purchase Zone Alarm or Comodo Firewall protection, the company will provide free antivirus with its product.

Thus, for $35–$60 a year you can obtain a reasonable level of protection against viruses, worms, Trojan horses, spyware, ransomware, and keylogging. These terms are all defined in the glossary, but the main thing to know is that these are all bad things that black hat hackers, or "crackers," can do to steal information from you while you are logged on to the Internet or using your smart phone.

The basic question that you must decide is which service to use. You might consult such trusted websites as Consumer Reports or AARP, but there is no specific "right" choice. The definitely wrong answer is to say I will take my chances and not get at least basic antivirus protection. If your funds are very limited at least opt to sign on with AVAST or Aviro.

Identity Theft Protection

The biggest nightmare that a person might encounter in today's cyber-world is identity theft. This means that someone not only takes over your identity but somehow manages to wipe out your bank account, switch your social security payments, or take out a large loan in your name for which you could be legally responsible unless you can prove the identity theft in court. Such identity theft can, and often does, occur online, but it can also happen by someone that targets your regular mail, your discarded but not shredded financial records, or by other means of eavesdropping. The most common means of identity threat, however, occurs online by intercepting passwords and accessing financial records via a keylogging program.

One might think that these are just isolated incidents that happen to only a few people, but a study conducted by Javelin Strategy and Research

concluded that 11.6 million Americans had some sort of identity theft issue during the course of a year. Other studies have projected different numbers of incidents, but clearly this is a widespread problem in the United States and around the world [3].

Fortunately protection is available against identity threat—and at reasonably low rates. These services typically cost between $125 and $330 a year and usually provide a $1 million warranty against financial loss due to identity theft. Below is an analysis of ten sites that provide identity theft protection and $1 million in insurance coverage. For more details, go to www.top10identitytheftprotection.com [4] (Table 2.3).

If you do sign up for identity theft protection we believe that the anti-keylogging/antivirus service is important to include, unless you already have this capability installed in your computer devices. The AARP service via Equifax is perhaps the lowest cost offering available, especially to seniors who are AARP members, but it is recommended that if one takes this service they have an antivirus service that protects against Internet hackers.

The types of services that can come with identity theft protection services varies a great deal. Lifelock, which actively markets its services via extensive television ads, offers services that range from $9.95 a month up to $29.95 a month. The range of services that are available is shown in the table below. Note, before you sign up, you should check carefully the range of services listed above, since these are given by the providers. Some of the providers have been sued for overstating their levels of protection. The chart below indicates a range of protective services offered by LifeLock that range from "Standard" to "Ultimate." Other providers offer alternative levels of protection. It is the opinion of the authors that most individual consumers that don't own businesses do not need to purchase higher levels of protection, but feel the $1 million service guarantee is key. Again, we are not endorsing LifeLock but merely citing its tiered level of protection as not untypical of identity theft protection services [5] (Table 2.4).

In making your actual decision about which service to select we suggest that you look at objective third parties in making your choice. Remember that those that advertise the most are not necessarily the best or cost effective. Three sites that you might consult in making your decision include:

http://www.consumeraffairs.com/privacy
http://www.thegeekprofessor.com/
http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/

Table 2.3 Identity theft services[a]

Service name/rating	Price	Fraud monitoring	ID theft insurance	Reports delivered	Computer security	Bottom line
Identity Guard	Free 30-day trial; $14.99/month (after our 25 % discount)	Monitors 3-bureau credit report, credit cards, public records, social security number, bank accounts, applications, Internet security	$1 million	3-bureau credit scores and a public record report each quarter	ZoneAlarm Internet security suite; anti-key-logging software	Most complete identity theft protection service we reviewed; 3-bureau credit report monitoring; credit report/score updates every quarter; 25 % discount and free 30-day trial
Trusted ID (AARP partnership)	Free 14-day trial and 10 % discount; $9.38/ month (paid annually)	Monitors 3-bureau credit report, credit cards, public records, social security number, bank accounts, medical records	$1 million warranty	Equifax credit reports and scores monthly; TransUnion, Experian credit reports and scores annually	None	Best value, especially for families; full credit report monitoring; monthly Equifax credit reports and scores; 10 % discount and free 14-day trial
AARP	Free 14-day trial and special AARP price; $9.17/ month (paid annually)	Monitors 3-bureau credit reports, bank accounts, credit cards, social security number, public records	$1 million service warranty	Equifax credit reports and scores monthly; Transunion, Experian credit reports and scores annually	None	Comprehensive identity theft protection and credit report monitoring for AARP members and family; monthly Equifax credit reports and scores; special AARP price and free 14-day trial
Lifelock Ultimate	Free[a] 30-day trial; $24.75/month (w/annual prepay and 10 % discount)	Monitors 3-bureau credit reports, applications, credit cards, social security number, driver's license, address change, credit card and bank account activity	$1 million guarantee	TransUnion credit scores monthly; 3-bureau credit reports and scores annually	None	Thorough identity theft protection and 3-bureau credit report monitoring; annual 3-bureau credit reports and scores; monthly TransUnion credit scores; somewhat costly even with 10 % discount; free[a] 30-day trial

Privacy Guard	30-day trial for $1; $14.99/month	Monitors 3-bureau credit report, Internet security	$1,000,000 insurance	All 3 bureau reports and scores monthly, social security report, medical info bureau report	Norton Internet Security Online	Solid credit protection with monthly credit report/score updates; includes our top-rated Internet security software; 30-day trial for $1
ID Freeze	Free 14-day trial and 15 % discount; $7.01/ month (paid annually)	Monitors credit cards, public records, social security number, bank accounts, medical records	$1 million warranty	All 3-bureau credit reports each year	None	Reasonably priced identity theft protection for individuals and families; doesn't provide credit report monitoring; 10 % discount and free 14-day trial
Lifelock	Free[a] 30-day trial; $8.25/month[a] (w/ annual prepay and our 10 % discount)	Monitors credit cards, social security number, driver's license on Internet black market and address change verification	$1 million guarantee	None, unless plan is upgraded	None	Valuable identity theft protection and customer support for an affordable price, yet lacks in terms of credit report monitoring; 10 % discount and free[a] 30-day trial
Legal Shield	$24.95/month and one-time $10 membership fee	Monitors 3-bureau credit report, credit cards, emails, phone numbers, Social Security number, bank accounts, medical records	None	All 3 bureau credit reports each year	None	Somewhat pricey when compared to other services; complete restoration assistance; no insurance/guarantee or security software
Protect my ID	7-day trial for $1 with enrollment in ProtectMyID; $19.95/mo	Monitors only Experian credit report, credit cards, new financial accounts or applications, address changes, public records	$1 million	One Experian credit report	None	An expensive option for ID theft protection and lacks in protection; only includes Experian credit report monitoring; 7-day trial for $1 with enrollment in ProtectMyID

[a]Table prepared by top10identitytheftprotection.com

Table 2.4 Example of typical service provider offering identity theft protection and other services

LifeLock protection features	LifeLock Standard	LifeLock Advantage	LifeLock Ultimate Plus
LifeLock Identity Alert® System	✓	✓	✓
Lost wallet protection	✓	✓	✓
Address change verification	✓	✓	✓
Reduced pre-approved credit card offers	✓	✓	✓
Black market website surveillance	✓	✓	✓
Live member support 24/7/365	✓	✓	✓
$1 million total service guarantee	✓	✓	✓
Fictitious identity monitoring		✓	✓
Court records scanning		✓	✓
Data breach notifications		✓	✓
Online annual credit reports and scores		1 credit bureau	3 reports
Credit card, checking and savings account activity alerts		✓	✓
Investment account activity alerts			✓
Checking and savings account application alerts			✓
Bank account takeover alerts			✓
Credit inquiry activity			✓
File-sharing network searches			✓
Sex offender registry reports			✓
Monthly credit score tracking			✓

Firewalls and Backup Memory

Corporations are now routinely using not only antivirus programs but firewalls as well. Most individuals rely on only antivirus protection, but corporations and individuals with home businesses feel this additional level of protection is useful. However, the protection as provided by personal firewalls can sometimes prove frustrating because you can be blocked from accessing sites like drop boxes that you actually wish to access.

A firewall is a coded protective barrier that separates a company's inside corporate intranet or your home-based "intranet" from the outside Internet or even your own smartphone in its most basic form. This typically allows effective and protected communications within a corporate environment, a home network, or just your desktop computer, tablet or smart phone. The idea is to create a barrier that "walls" you off from the Internet so that you have a filtered screen that keeps out harmful external communications.

A protected intranet, even with a sophisticated corporate firewall, is still no guarantee of absolute protection. If a telecommuting employee is at home, logs in, and then connects to an unprotected wireless LAN, then

security is breached. Anyone with a scanner can eavesdrop via this open and unprotected access to the corporate network. Firewalls can also be penetrated by expert "crackers."

The following analysis from Brighthub indicates both the pros and cons of personal firewall protection [6].

Common Features That Personal Firewall Can Offer

- It can help protect the user from unwanted incoming connection attempts—especially by spyware and keylogging software.
- A firewall generally allows the user to control which programs can and cannot access the local network and/or Internet. It typically provides the user with information about an application that makes a connection attempt.
- A firewall also can block and alert the user about outgoing connection attempts from within a local area network. (This is the case if the firewall is actually serving multiple computers rather than a single computer.)
- A firewall serves to hide a computer from port scans. This is accomplished by not responding to unsolicited network traffic.

The main function of the firewall is to monitor and regulate all incoming and outgoing Internet users and their traffic. It thus should prevent all unwanted network traffic from being able to affect (or infect) locally installed applications.

Limitations of Firewalls

- If the system has already been compromised by malware, spyware, or keylogging software, these programs can also potentially manipulate the firewall. This is because they are both running on the same system. It may be possible to bypass or even completely shut down software firewalls, depending on their design.
- If a firewall has initially been incorrectly configured, this will not be obvious to the user.
- Firewall may limit access from the Internet, but it may not absolutely protect your network from wireless LAN access or and other access to your systems.
- Firewalls and virtual private networks are not the only solution to secure private documents and e-mails. Encryption or other techniques can be used.

- The frequent alerts that can be generated by firewalls can over time make users less vigilant concerning actual malware attacks.
- Software firewalls that interface with the operating system or with other firewalls or security software at the kernel mode level to allow backdoor access could potentially cause instability and/or introduce security flaws.

Large corporations with many users, such as airlines, large retailers, or credit card companies, hire "white hat" hackers to try to penetrate their firewalls in order to better protect themselves and bolster the protected shield of their firewall. Not all computer adept hackers are bad guys! The U. S. Cyber Command and lots of other units in the United States and around the world are using their white hat skills to protect against viruses and other malware that attacks the Internet and governmental and corporate databases and networking services.

The pricing for a firewall depends on the amount of traffic in and out of a computer or a computer intranet within a corporation or enterprise network. Individuals with personal firewalls would thus get protection at a relatively low rate for a small amount traffic that is equivalent to the cost of an antivirus. Some vendors offer free antivirus software with a firewall, for instance.

Large global corporations with so-called enterprise networks will pay thousands of dollars for firewall protection. Such corporations or governmental agencies, of course, typically also pay for back-up memory to store and protect vital data in a highly secure site. Today corporations often use the Cloud for storage and secure processing, but individuals should be sure the Cloud that is accessed is completely secure and backed up and well protected against cyber-attacks.

A 2013 assessment by NSS Labs of Next Generation Firewall (NGFW) systems for enterprise networks concluded that these products continue to improve in terms of qualitative performance. The NSS ran a series of demanding tests that gave recommended status to eight out of the nine systems listed below in terms of performance, but gave an unexpectedly low rating to the Palo Alto system. It also reported that there is a still a significant range with regard to the cost of protection. The NSS Labs report found that the Next Generation Firewall protection rates (per 1 megabit/s data streams) ranged for a low of $18 per 1 mbps to a high of $125 per 1 mbps (Table 2.5).

If one might doubt why such a sophisticated firewall is essential for corporations and individuals in today's universally accessed cyber world, you need only to recall the Sony hacking incident. This malicious cyber-attack mounted by North Korean sponsored hackers almost brought this media giant to its knees. It did not put Sony out of business, but the losses were in the millions of dollars and the exposed confidential messages led to enormous embarrassments and even suits against Sony by its clients and superstars.

Table 2.5 Assessments of firewall effectiveness

NSS next generation firewall comparative analysis reports	
Next Generation Fire Wall	Rating results
Check Point 12600	Above 90 % and recommended
Dell SonicWALL SuperMassive E10800	Above 90 % and recommended
Fortinet FortiGate 3600C	Above 90 % and recommended
Juniper SRX 3600	Above 90 % and recommended
Palo Alto PA-5020	Not recommended
Sourcefire 8250	Above 90 % and recommended
Sourcefire 8290	Above 90 % and recommended
Stonesoft 3202	Above 90 % and recommended
WatchGuard XTM 2050	Above 90 % and recommended
Go to NSS Lab site to find out how to get the detailed NSS Labs assessment: https://www.nsslabs.com/next-generation-firewall-reports	

Insurance Offerings

One can go beyond obtaining an antivirus, identity theft protection, or firewall system in order to isolate your network from intrusions. In this case you are seeking a comprehensive overall set of defense systems against all conceivable types of computer attacks. This can include such aspects as protection against cyber-bullying, junk mail, or loss of your purse or wallet.

In short there is a comprehensive approach to network security, identity theft, phishing, pharming, and any other possible form of cyber-attack on you, your family, or your assets—comprehensive data protection services in the form of an insurance policy. The MetLife Defender, for instance, provides this comparative analysis of their service versus a "typical" identity theft protection service. MetLife is, of course, just one such provider of this comprehensive insurance coverage. Again we are not necessarily endorsing Met Life. You should go to independent consumer advisor sites for help in making your decision. Again these sites include [7] (Table 2.6).

The insurance policy approach has its advantages in being comprehensive and providing cash compensation if something goes wrong, but it can also be expensive. Many such financial data production plans are available through employers, however, and thus at substantial discounts. A number of the antivirus, firewall, or malware protective services do offer up to $1 million in protective compensation against intrusions. If you are an individual the minimum protection that we recommend is an antivirus with a reasonably good rating and one that can allow you protection on all of your devices that connect to the Internet. Unfortunately, as we enter the age of the Internet of Things, you may have a number of appliances or devices in

Table 2.6 Comparison of comprehensive insurance offering from MetLife

Feature/benefit	MetLife defender	Typical ID theft protection services	Typical financial institutions	Typical credit monitoring services
Financial data protection comparison				
Patented multi-account financial protection	Y	N	N	N
Credit monitoring	Y	Y	N	Y
Lost wallet protection	Y	Y	N	N
Identity theft and personal data protection comparison				
25 data point personal identity monitoring and security	Y	N	N	N
Patented deep internet protection	Y	N	N	N
Privacy protection	Y	Y	N	N
Junk mail removal	Y	Y	N	N
Health data monitoring comparison				
Medical insurance fraud protection	Y	N	N	N
Health and medical data protection	Y	N	N	N
Online child safety comparison				
Child identity theft protection	Y	Y	N	N
Cyber predator detection and notification	Y	N	N	N
Cyberbullying applications and scanning	Y	N	N	N
Additional features comparison				
24/7 service & support	Y	Y	Y	N
Proactive alerts	Y	Y	N	N
Theft and fraud resolution service	Y	Y	N	N
Service guarantee	Y	Y	Y	N

your home or car or truck that link to the Internet without you even being aware of these connections. In this case we will likely need legislation to force manufacturers to provide antivirus protection so that netbots cannot be used against you or others.

What to Do

There are many practical steps that you can take to protect yourself. The minimum is a basic antivirus program. The antivirus that is often rated the most highly in terms of performance and cost is McAfee by Intel Security. Avast and Avira are the most widely used of the free antivirus offerings, but the *PC Magazine* website reviews all such offerings. From there one can consider obtaining a firewall and identity theft coverage. An identity theft protection plan such as the AARP offering in collaboration with Equifax is available

to AARP member at just over $100 per year, but there are many packages that are available for a similar price that are likely comparable in coverage areas.

There are also minimum-level protection alert systems against identity theft or credit alerts.

Some companies such as ID Safe or AllClear ID offer free, bare-bones versions of identity theft protection services that monitor the Internet for hints that your personal particulars are for sale. These services would normally include monitoring of three credit cards to determine if the numbers are being sold on the black market plus a free annual credit report and score.

IDSafe or AllClear by Debix can also help you close accounts that have been attacked, place fraud alerts at the big credit bureaus and assist with the financial damage to help you restore your credit if your identity is indeed stolen. All of these services, just as in the case of Avast.com or Avira.com that provide "free antivirus," seek to upgrade you for a paid version that would typically cost $15 a month [8].

As noted at the outset of this chapter a full range of protection against computer viruses, a firewall, and up to $1 million in identity theft protection is available for substantially less than a year's subscription to the *Washington Post, The New York Times*, the *Chicago Tribune* or the *LA Times.*

At the top of level of personal cyber-protection coverage is a comprehensive "insurance policy" like the MetLife Defender. Corporations in today's world must recognize that their databases, key intellectual information, billing systems, etc., are their most valuable resources. Protection of these resources via all forms of cyber-defenses, including high quality encryption, is necessary in today's world. This book is focused on the individual. But if you own your company or work for a corporation, you should make sure that you have a full range of cyber-defenses in place as well. In the chapter on the future we will examine in more detail new ways to protect government databases and companies that operate vital infrastructure. These cyber-protections are now key to families, businesses, and national security.

And Now How to Protect Your Family Against Cyberbullies, Pornography, Online Hate Messages, and Other Cyber-Related Maladies

First, there is the straight talk message that protecting you and your family against unwanted content over the Internet is difficult, and law enforcement officials are often slow to respond to help and in addition are limited in the laws that they have at hand to enforce. Further, the most heinous and

hurtful trolls, spinner of false talks, purveyors of hate crimes, and distributors of pornography hide behind anonymous web names and unidentifiable web domain names to avoid criminal prosecution. Blocking purveyors of hate messages and pornographers and legally prosecuting them or shutting them is, unfortunately, hard to do.

The reasons why cyberbullying, hate messaging and pornographic distribution is so hard to get rid of are anonymous websites, web postings, and aliases. Thus the attackers and trolls are often "ghosts," and, as you can see from the list below, it is hard to locate these spectral beings that only exist online and accordingly can hide their real identity.

1. Many of the most offensive websites and sources of hate crime messages and pornography operate from offshore sites outside of the United States, Europe, or other countries that have enacted laws to prosecute cybercriminals and techno-terrorists.
2. Targeted individuals are often frightened by such attacks and are reluctant to bring the offensive language, false profile, or Photoshopped™ image to the attention of parents, school officials, or the police. A young girl who has had their face pasted on the provocative nude image of a Playboy Playmate may be too embarrassed to report this to their parent or school advisor.
3. There are a lack of effective laws and ordinances that allow criminal prosecution of offenders. And court cases take time and money to pursue. While a legal case is going through a prosecuting attorney's office and through a trial, the offending material could well remain online.
4. Many cyber-attacks are protected by freedom of speech and the right to express oneself openly in democratic societies.

And the problem is not a minor issue with people affected by malicious cyberbullying or hate crime attacks. The *2013 Youth Risk Behavior Surveillance* Survey finds that 15 % of high school students (Grades 9–12) were electronically bullied in the past year. It is noteworthy that there was a wide variation in gender of those actually bullied, namely 21 % of girls but only 8.5 % of boys [9].

The *Journal of the American Medical Association* found 50 % of children have been asked to send revealing or even nude pictures of themselves over the Internet, a practice now widely known as sexting. In a world filled with X-rated videos, adult video channels, and cable television channels in many homes with pornographic programming, it is hard for young people to understand what is wrong with sharing racy photos or even nude images.

Even if there is no such programming in your home or V-chip restrictions on adult programming, this type of programming is likely available at a friend's home instead [10].

According to interviews conducted by Pew Studies and media-sponsored surveys, only 50 % of parents talk with kids about avoiding these encounters. Teens in particular try to cope on their own. This can result in retaliatory behavior that can put youths even more at risk, or can let a problem grow out of control. By the time adults, scholar advisors, or even police become involved in Internet-based controversies hundreds if not thousands of others have become targets of cyber-attacks that may involve false profiles, allegations of wrongdoing or other hurtful information being spread via text, social media, or website postings that could ultimately hurt your offspring's chances when it comes to college admissions or job interviews.

And it should be noted that the problems of the cyber-world continue to expand as we become more and more dependent on our "intellectual prosthetics." Today our "smart" computers, laptops, and interactive smart phones can provide almost any requested information on instant demand. With hundreds of apps now available to us, there can be a loss of spelling, math, or reasoning skills. Most young people today who rely on texting to communicate do not know how to write cursive, spell words, and are starting to lose basic skills in mathematics. In a world where "spell check" and "smart phone" and other intellectual prosthetics hold sway there are concerns that this loss of skills that is sometimes called "de-skilling" will exacerbate the problem of competing in a global information services market. Copyediting, inventory control, back office accounting, and software development can now be done (if poorly) by anyone in the world with a communications link and computer (Fig. 2.1).

What to Do About Protecting Your Family's Computers from Cyber Criminals, Stalkers and Bullies

The first thing to do is to recognize that these are real problems that are quite common. You need to assume that various types of cyber difficulties will actually arise for your kids, your spouse and/or elderly parents or relatives. You need to talk to them and warn them of potential problems that can arise and are now common they are now around the world. As noted in the above studies by many reputable research organizations cyberbullying

Fig. 2.1 Problem of de-skilling is yet another worry that comes with the computer age (Graphic provided by the author J. Pelton from his book *Future View.*)

via social media, texting, and other electronic means is a growing problem, and because of the Internet more people can be exposed quickly and the harm can be enormous. It has alarmingly led to a rash of suicides in countries around the globe.

Fortunately there are videos and online materials that can help spell out the problems, potential solutions, and websites and services designed to assist with these various cyber problems. The following table indicates recommended videos, websites, and services designed to cope with cyber problems associated with teens and "tweens" (those not quite teens, or in U. S. parlance, "middle schoolers"). These sites and services can also assist parents in coping with cybersecurity and especially cyberbullying problems involving their children. There are a growing number of services that address not only cyberbullying but also monitoring smart phone usage and restricting viewing patterns for kids (Table 2.7).

Table 2.7 Available websites, services, and videos that you and your family might use to find advice about cybersecurity and cyberbullying

Federal Bureau of Investigation (FBI) Video on Cybersecurity Go to: https://sos.fbi.gov This website offers fun, age appropriate lessons (3rd grade up) about cyber safety. The exercise included is based on an interactive island exploration game. It is an educational game and definitely more fun and interesting than listening to another safety lecture from an adult.
Sponsored by Trend Micro "Cybercrime exposed: how to spot a phishing scam" A 2:20 min. video on youtube.com Go to: www.youtube.com/watch?v=pXp2RvA0SBU
Sponsored by AVIRA SocialShield Avira.com "How to Protect Your Kids on Social Media," A 3:27 min video for parents. (Note Avira.com is one of the providers of a "free" antivirus service along with Advast) Go to: www.youtube.com/watch?v=IRlAMMaNr8U
Federal Trade Commission (FTC) "Stand up to cyberbullying" (1:20 min) Go to: www.youtube.com/watch?v=lN2fuKPDzHA
BRIM website Go to: https://stopbullying.gov This site provides useful tips about how to cope with various attempts at cyberbullying and strategies that can help protect children. This you should view with your children and answer their questions.
HIBSTER website Go to: http://hibreporting.com This website is an active anti-bullying program that specializes in incident prevention, management, and reporting.
STOPIT Go to: http://stopitcyberbully.com How to report, track and effectively deter cyberbullying in your school and neighborhood. When a child on "StopIT" sees something online that's not okay, whether directed at that person or a friend or peer he or she can immediately use the STOPIt app to let a trusted adult know right away what the cyberbullying message is about. Those signed up for "StopIt" can send messages and/or screenshots directly to the trusted adult(s) such as a parent, aunt or uncle, grandparent, or school counselor. This can even be sent anonymously to alert a responsible adult. Details on enrollment are pending shortly.
App Certain Go to: https://www.appcertain.com Cost: Free App Certain will e-mail parents when their child downloads a new app, and will provide an analysis about that app like if the app has expensive in-app purchases or accesses your contact list. Parents can also utilize a "curfew mode" that gives the remote access the ability to turn off their children's access to their apps and games at a certain time.
Mobile Watchdog Go to: https://www.mymobilewatchdog.com/default.shtml Cost: Free for 14 day trial and then $4.95 per month, with cancelable service at any time. Allows users to monitor all cell phone activity on Android and I Phone devices—text messaging, application use, and browsing use. You can program in special words and be alerted if these words appear in a text or e-mail. This app will send you an e-mail reporting on a child's mobile phone activity. It does not have a "stealth operating mode" for listening in on cell phones.

What to Do About Pornographic Sites and Sexting

There are many services that can introduce monitors for smart cell phones and use browsers that are geared not to access X-rated or pornography sites. Some of these are noted in the table below. The problem is that even if V-chips are used to block out pornographic cable television channels and some of the services such as K-9 Browser, young and impressionable youths can be exposed to nudity, sexual videos, and other undesirable behavior through the smart phones of friends or computers in other houses. The survey conducted by doctors for the *Journal of the American Medical Association (JAMA)* about sexting and teen sexual behavior is indicative of the contemporary sexual environment is in the United States, which is probably not greatly different from other OECD countries. This particular study found that nearly 25 % of 16-and 17-year-olds had experienced sexting on the sending or receiving end. Further its findings indicated that those who had engaged in this practice were twice as likely to have engaged in sexual intercourse (i.e., 77 % versus 40 % of those that had not sexted) [10].

This is simply to say that monitoring and controls can only go so far to protect children—particularly when they reach a certain age. Once children reach perhaps 13 or 14 years old such controls really can easily be avoided by enterprising youngsters. If they feel they are being overprotected or their viewing habits unduly restricted this might well lead to rebellious behavior. Good and trusted communications between parents and offspring and a good academic environment with trusted teachers are key to healthy development. It is really a matter of instilled values, and trustworthy friends and siblings, rather than imposed limits once a tween approaches teenagehood (Table 2.8).

Protective Strategies for the Over-50 Crowd

One can surf the website of the American Association for Retired Persons (AARP) and find a number of very useful tips and strategies on digital privacy, cybersecurity, backing up vital information stored on computer hard drives, and protecting against phishing, pharming, ransomware and identity theft. These can be summarized in the following list.

Table 2.8 Services to restrict access to pornographic sites and monitor smart phone usage

K-9 Browser Cost: Free This provides a specially designed and highly rated browser that children can use instead of an Internet browser that goes to all possible sites. This browser with this special app will block adult content. It's available for the iPad, iPhone, iPod, Android, and a desktop computer. The difficulty is to ensure that children consistently use this browser and not Yahoo, Google, or another browser with no screening capability.
Net Nanny Cost: See website for details This service can be installed on I-Phones and Android phones for various annual fees ranging from a low of about $5 up to $20 for Net Nanny Social. Net Nanny has mobile monitoring services for Android and Apple that will help block adult content. It also offers Net Nanny Social, which installs special software to screen for cyberbullying or unsafe activity. If anything unsafe is detected, parents receive an alert. Parents can also log in and see all social media activity in a Cloud-based dashboard on any device.

1. Protect the data, photographs and key documents that you have stored on your computer's hard drive. As noted on the AARP site, your computer's hard drive, because it is a mechanical device, will ultimately fail. You can key keep a lot of key information on a thumb drive (also known as a flash drive), but this can't store everything. There are lots of high density hard drives (portable storages of several hundred gigabytes and desktop units of several terabytes). These run from $50 to $200 (e. g., Seagate, Western Digital, etc.). Or there automatic backup services that you can sign up for a small annual fee [11].
2. It is particularly important to protect against identity theft and to avoid the problems that can come with the theft of credit card numbers and codes, Social Security numbers, or Medicare and medical records. AARP articles highlight that 16 million people in the United States alone fall victim to identity theft, and that those over 50 are often sought out as prey for cyber criminals. AARP research notes that this is not always cyber theft, and highlights that only one in five people shred documents that could be used to steal their identity. It is interesting that articles on the AARP site explain that there are "free" services such as ID Safe and AllClear that provide a "bare bones" service, even though AARP itself provides a discounted rate for identity theft in its partnership with "Trusted ID." This is for a more robust service that has been given top ratings by independent reviewers, as noted in the table above [12].
3. It is important to install antivirus and a basic firewall on your computers and electronic devices, including your cell phone. Also make sure your wireless router is password protected, and don't go to sites that your antivirus software warns you not to go to [13].

4. Take special care to protect your "smart phone." One in three robberies net a cell phone. "Apple Picking" (or theft of I-Phones) is by itself a huge industry. A particularly useful AARP article outlines 12 ways to protect your smart phone [14]. Also you should be careful about how you sign up for and protect the insta-payment systems that are installed on your cell phone in terms of tap and go or swipe and go systems. (Note: These issues of cell phone security and touch and go systems are discussed in further detail in Chap. 5.)
5. Use social media wisely. Social media is a great way to interact with family and close friends, but be careful about posting too much personal information on your website that might be used by cyber criminals. This information might not only be used to try to get money or assets from you and your family, but it might also be used in phishing or pharming schemes to make a request to friends or family for money. If a cyber-criminal is armed with enough personal knowledge of you and your habits that person might exploit unsuspecting close associates of yours [15].

Conclusions

If there is a vital message in this entire book, it is the following words of advice and counsel. The Internet, the world wide web, hyperlinks, social media, smart phones, texting, mobile apps are wonderful new tools of our times. These tools let us stay in touch with family, friends, and loved ones, buy what we need on the go, and live a more convenient and free-wheeling life. Electronic media and communications devices keep us educated, informed and up-to-date in ways that were never before possible in the entirety of human history. The amount of information that we can obtain, store and access is greater than ever before, and the cost of storage, processing, and imaging keeps falling as new computer and communications technologies move forward.

There is, however, a cost associated with the use of these electronic tools, one that we must pay to insure that we maintain our privacy, protect ourselves from identity theft, and increase the security of our family and loved ones. We must invest in protective systems and cybersecurity tools in order to ward off the various malware and viruses and worms that cyber-criminals might employ when they seek to infect our computers, laptops, tablets, smart phones, and other electronic gizmos.

In a word, you really need to obtain help from various vendors of protective services, consistently use and protect well-crafted passwords, and back up important and sensitive data against computer failure as well as to protect against an attack by a computer virus. For much less than what one might pay each year for a newspaper subscription, you can get a range of protective services as well as systematic help with other cyber-related problems such as cyberbullying, children accessing pornographic sites, etc. This is the trade-off. On one hand you can access a great deal of information and images and advice for free. In order to ensure that some of that information is not a harmful attack on you and your computer or smart phone you must wisely follow the advice provided to you in this chapter and sign up for cybersecurity services.

If your budget is particularly tight then at least avail yourself of free services such as those provided by Avast, Avira, IDSafe and AllClear. There are lots of helpful websites out there to aid you in making good choices. The main thing is not to delay putting protective cybersecurity systems in place. Also, you should follow other good privacy and security practices such as protecting your mail, shredding your financial and other personal records, and making sure your various important financial, medical, and personal passwords are backed up and well protected.

We can't cover every issue in one short book, but we hope this chapter in particular has started you on the way. Remember, there are lots of good and useful websites out there as well as public librarians and other public servants that can provide useful and timely advice.

References

1. Norton Internet Security www.Symantec-Norton.com/Security.
2. "Top Ten Antivirus Sites" Matchtop.com. http://antivirus.thetop10sites.com/?matchtype=b&keyword=norton%20antivirus%20vs%20mcafee&adposition=1t1&creative=60402236670&aceid=&gclid=CMm88LWgh8MCFQhk7AodN3AASg#gsc.tab=0.
3. 2012 Identity Fraud Survey Report. Javelin Strategy & Research. February 2012.
4. "Top Ten Identity Theft Protection Sites." www.top10identitytheftprotection.com.
5. Life Lock Individual Plans: Identity Theft Protection, http://www.lifelock.com/services/.
6. Daniel Brecht and edited by: Bill Bunter, "Pros and Cons of Computer Security Systems" http://www.brighthub.com/computing/smb-security/articles/32411.aspx also see. Finn Orfano and edited by Bill Bunte, "Firewall Basics Part III: The Pros and Cons of Firewall Methods." http://www.brighthub.com/computing/smb-security/articles/8293.aspx.

7. MetLife Defender. https://www.metlife.com/individual/employee-benefits/metlife-defender/index.html.
8. "She Stole My Life," *AARP Magazine,* Nov. 2014.
9. "2013 Youth Risk Behavior Surveillance Survey, Centers for Disease Control and Prevention," June 13, 2014.
10. Jeff R. Temple, Ph.D., Jonathan A. Paul, Ph.D., Patricia van den Berg, P.hD., Vi Donna Le, B.S.; Amy McElhany, B.A.; Brian W. Temple, M.D. "Teen Sexting and Its Association With Sexual Behaviors," *Journal of the American Medical Association,* September 2012, Vol. 166, No. 9 http://archpedi.jamanetwork.com/article.aspx?articleid=1212181.
11. Gary M. Kaye, "Sooner or Later Your Hard Drive Will Fail: Computer backup is like digital fire insurance" AARP, June 23, 2011. http://www.aarp.org/technology/privacy-security/info-06-2011/back-up-computer-files.2.html.
12. Gretchen Anderson "Identity Theft: Who's At Risk?" AARP Research, September 2014. http://www.aarp.org/money/scams-fraud/info-2014/identity-theft-incidence-risk-behaviors.html.
13. Kim Loop, "Prevention, Not Just Awareness, Key to Cyber Security." AARP Texas October 11, 2012. http://states.aarp.org/prevention-awareness-cyber-security/.
14. Sid Kirchheimer, "Scam Alert: How to Cyberproof Your Phone – 12 ways to protect yourself and your device," AARP Bulletin, May 2014 http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html.
15. Technology, Tablets, and Social Media. http://states.aarp.org/prevention-awareness-cyber-security/.