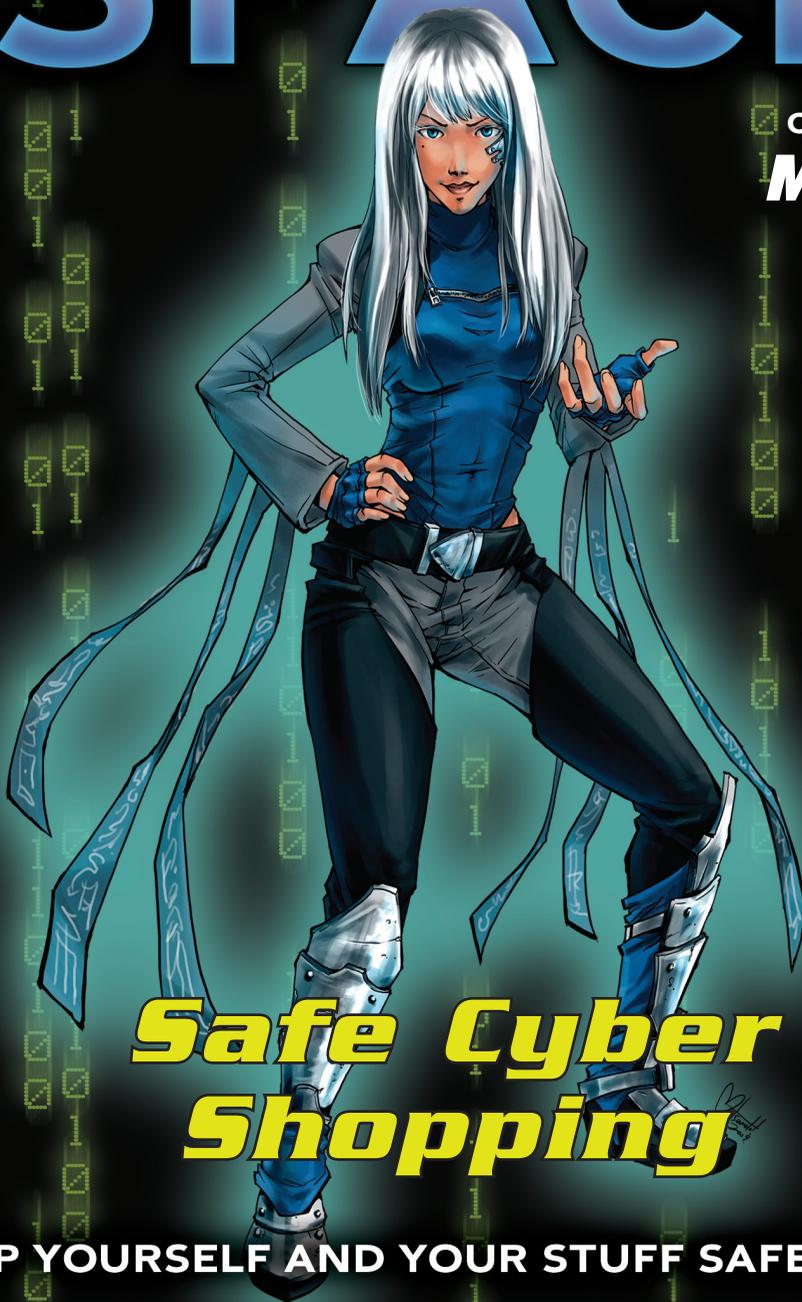


OWN YOUR SPACE

Compliments of
Microsoft



***Safe Cyber
Shopping***

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE



Edited by Linda McCarthy and Denise Weldon-Siviy

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein. All trademarks are the property of their respective owners.

Publisher: Linda McCarthy
Editor in Chief: Denise Weldon-Siviy
Managing Editor: Linda McCarthy
Cover designer: Alan Clements
Cover artist: Nina Matsumoto
Interior artist: Heather Dixon
Web design: Eric Tindall and Ngenworks
Indexer: Joy Dean Lee
Interior design and composition: Kim Scott, Bumpy Design
Content distribution: Keith Watson

The publisher offers printed discounts on this book when ordered in quantity for bulk purchases, or special sales, which may include electronic versions and/or custom covers and content particular to your business, training, goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Education Sales
(510) 220-8865



Except where otherwise noted, content in this publication is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License, available at <http://creativecommons.org/licenses/by-sa/3.0/us/legalcode>.

ISBN 978-0-615-37366-9

Library of Congress Cataloging-in-publication Data

McCarthy, Linda

Own your space : keep yourself and your stuff safe online / Linda McCarthy.

ISBN 978-0-615-37366-9 (electronic) 1. Computer security. 2. Computers and children. 3. Internet and teenagers. 4. Computer networks--Security measures. I. Title.

Visit us on the Web: www.100pagepress.com

Download free electronic versions of the book from MySpace (<http://www.myspace.com/ownyourspace>) and Facebook (<http://www.facebook.com/ownyourspace.net>), and from Own Your Space (<http://www.ownyourspace.net>)

Chapter 8

Safe Cyber Shopping

Meet Frank Wong, a 15-year-old cyber-shopper from Cleveland, Ohio. Frank began his online commerce experience when he used his mom Sally's credit card to open his Xbox 360 account. A few weeks later, Sally was blown away when Frank asked if he could buy his T-shirts online. The mall didn't carry the cool shirts that Frank wanted. Buying Frank's shirts online saved Sally a trip to the mall and she's been happy to have Frank purchase his own T-shirts, books, and other supplies online. Sally hates the mall.

Frank still can't remember the combination to his school locker. But he has memorized Sally's Visa number, even the expiration date and verification code! Sally's not all that thrilled about his ability to memorize her credit card information, but she loves shopping online.



Except where otherwise noted, content in this publication is licensed under the Creative Commons Attribution-NonCommercial-No Derivative Works 3.0 United States License, available at <http://creativecommons.org/licenses/by-sa/3.0/us/legalcode>
ISBN 978-0-615-37366-9

This year, Sally will be far from the only mom—or dad—skipping the mall for the convenience of shopping online. **eCommerce** has become a major part of the American consumer experience.

eCommerce Electronic commerce. The business of buying and selling stuff online.

A mere decade ago, online shopping seemed the province of upscale professionals and the technological elite. No more. Today, grandmothers and programmers alike peruse Amazon and eToys for that perfect birthday gift. The ranks of eBay users have also swelled to include a substantial percentage of holiday shoppers.

At first glance, online shopping seems one of the few areas where teens aren't leading the pack in Internet usage. Internet shopping is actually highest among those people demographers call Gen X and the Millennials. Gen X includes those people born from 1965 to 1976, 80% of whom shop online. The Millennials are those people born from 1977 to 1990. 71% of them shop online. In contrast, only 38% of users under 18 shop online. Sort of. The biggest difference between teen users and their X-men or Millennial elders is actually who's holding the credit card. Teens under 18 who shop online are obviously doing so with someone else's credit card. When you factor in the number of teens who receive goods bought online which they actually picked out themselves but had a parent order, you get a much higher percentage of online shoppers.

As online shopping has taken off, the general public has also become more aware of both privacy and security issues. Sending credit card numbers and **eChecks** makes some people a bit paranoid. An eCheck is an electronic version of a bank check. Unlike a money order (which is a check-like piece of paper that anyone can buy using cash even if they don't have a checking account), an eCheck is tied to a specific bank account just like a real check. It simply exists only electronically, not on paper.

eCheck An electronic version of a bank check.

eCommerce should make people a little nervous, but within reason. Although online fraud has expanded along with eCommerce, online paranoia has expanded even faster. Should you be careful about shipping off your parents' Visa numbers

to perfect strangers? Absolutely! Is this really more dangerous than handing their credit card to another cashier at the mall? Maybe not.

Obviously, there are real dangers and risks in using those Check Out options on the Internet. But it's important to put those dangers in perspective. In this chapter, we'll examine the real risks of online commerce and talk frankly about how to minimize those dangers while taking advantage of the wonders and freedoms provided by putting the world's malls at the tip of your keyboarding fingers.

8.1 Online Shopping Basics

As reliable broadband service has become available to most American consumers, the number of online shoppers has skyrocketed. Cyber Monday is now as much a part of our holiday season as Black Friday, and gaining on its predecessor. In 2009, Cyber Monday sales topped \$887 million. Amazingly, that wasn't even a record-setter for a single day's online sales. That record is currently \$913 million in sales recorded on December 15, 2009. That's nearly a billion dollars in online sales on a single day!

Online shoppers now fall into nearly every age range and most socioeconomic groups. Obviously, the poorest shoppers account for far fewer online purchases. Of course, they also account for far fewer purchases of any kind. Surprisingly though, the highest sales came from middle-income rather than the most affluent shoppers. Price-conscious netizens are especially pleased with the experience, using Search engines and comparison shopping sites to get the most bang from their shopping buck.

The spread of faster broadband connections has also had an effect on online purchases. No longer forced to wait for detailed photos or websites to download, broadband users account for the vast majority of online purchases.

Gender Gap

When it comes to Internet usage, there really is a gender gap—but probably not the one you'd expect. The heaviest users by far of most Internet services are older teenage girls.

Fifteen- to seventeen-year-old girls out-communicate all age groups online, with **97%** using IM versus only 87% of boys the same age. And, girls set the highest rates for seeking online information about everything from college options to religion and favorite movie stars!

The number of online shoppers is likely to continue growing. Several studies have found that once a consumer makes a “good” online purchase, she’s very likely to make more and more purchases online. And, despite concerns over on-

Looking for a Better Deal?

Easy comparison shopping is one of many areas where online commerce beats the socks off traditional brick and mortar establishments. To compare prices on your upcoming purchases, try one of 2009’s top comparison shopping sites:

- NexTag
- PriceGrabber
- PriceRunner
- Pronto.com
- Shopping.com
- Shopzilla
- StreetPrices.com
- Yahoo Shopping

line scams and identity theft, most online purchases are good. A full 80% of shoppers were satisfied with their latest online purchases. Online sales offer incredible convenience—particularly when Mother Nature doesn’t. When blizzards hit the East Coast in mid-December of 2009, online sales hit \$4.8 billion for a single week.

8.1.2 What Are They Buying?

Mention online buying to an average newbie and you’re likely to get a comment about eBay. While the online auction giant is still the place to go for obscure teacups and collectibles of any genre, eBay no longer rules the roost in online sales. By 2010, the top markets included fixed price offerings by both eCommerce only sites and online versions of traditional chains.

So what are shoppers buying online? Almost everything:

Electronics and Computer Goods

As you might expect, electronic goods sell briskly online. After all, these are the goods specifically targeted to the most technologically savvy online users.

Clothing

When LL Bean and Lands’ End began offering online shopping to traditional catalogue customers, they began a trend that still shows no signs of abating. While LL Bean and Lands’ End still dominate in this market, they’ve now been joined by Old Navy, Gap, Hot Topic, Forever 21, Delia’s, Hollister, Pac Sun, and Victoria’s Secret.

Books

Sales of both new and used books have also surged online. Amazon leads the pack, but a wide variety of challengers (Barnes and Noble, Borders, Abe Books, etc.) follow with strong sales figures. Amazon, of course, sets some pretty astronomical figures to follow. Amazon media sales topped \$12 billion worldwide in 2009. Although not all of those purchases were books (“media” includes books, music, and DVDs), that’s still a lot of happy readers!

Almost Anything Else

For obscure items in almost any category, eBay still leads the pack. While eBay has taken on almost mythic proportions in pop culture, its real presence is still pretty impressive. During just the last quarter of 2009, over \$2.04 billion dollars worth of goods were traded there. Altogether, eBay’s 90 million registered users bought \$2,000 worth of goods every second during 2009. Incredibly, that was a decrease from 2008, reflecting the general downturn in the economy.

eBay has also been getting some competition from craigslist, a service that offers free postings to would-be sellers and traders.

For the not-so-obscure items, let’s not forget Walmart. They offer a wide range of ordinary, general merchandise online. In July 2009, Walmart.com had over thirty-two and a half million visitors.

8.2 Shopping Problems

Although 80% of online shoppers have been happy with their experiences, there are still a number of pitfalls to be navigated in the commercial corners of cyber space. The most important, to most users, are understanding (and avoiding) data pharming, and protecting yourself from both online fraud and identity theft.

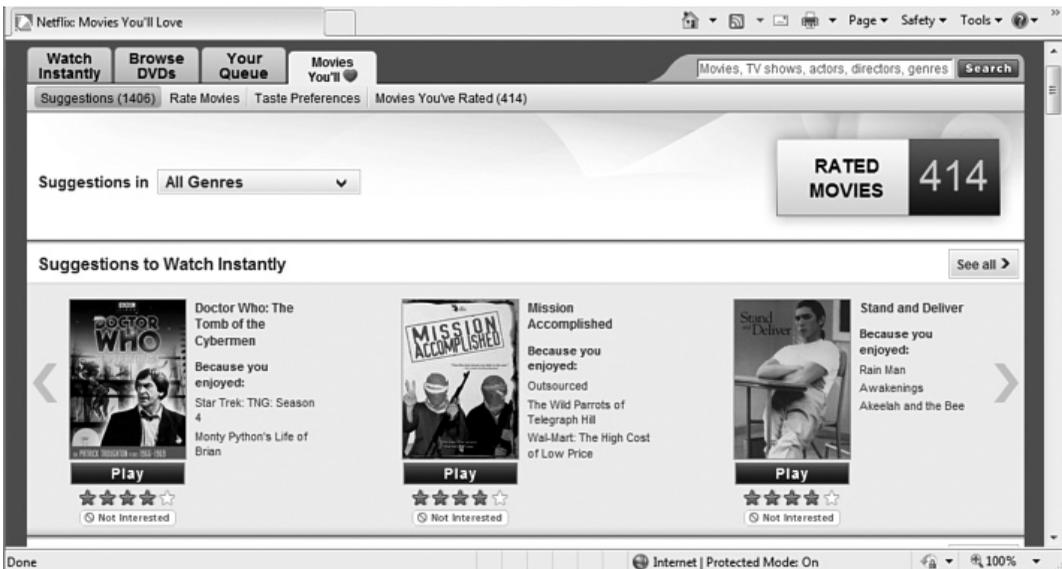
8.2.1 Data Pharmers

Data pharming is one of the dangers of shopping, or even browsing, online. Simply put, a data pharmer is someone who farms the Internet, growing collections (databases) of information about Internet users.

This isn’t always a bad thing. Some of the biggest names in online retailing collect a great deal of information about their buyers. These legitimate users never use

the term “data pharming.” Instead, they “track preferences.” Consider Amazon. If you’re an Amazon buyer, chances are that Amazon knows a good bit about you and your online buying habits. They keep track of what you look at as well as what you buy. They track your purchases and even use that data to suggest other items that you’d probably be interested in. If you buy one book in a series, Amazon lets you know when the next book in that series is released.

Netflix, the online movie rental company, does the same. When you rate movies on the Netflix site, they compile your ratings and use those to recommend similar movies that you’d probably like.



Often, this preference tracking can work to your advantage. We’ve found that over 75% of the movies that Netflix thought we’d love were films that we’d already seen and liked or had planned to see eventually. Likewise, we’ve ordered at least a handful of Amazon’s suggestions and been quite pleased with the results.

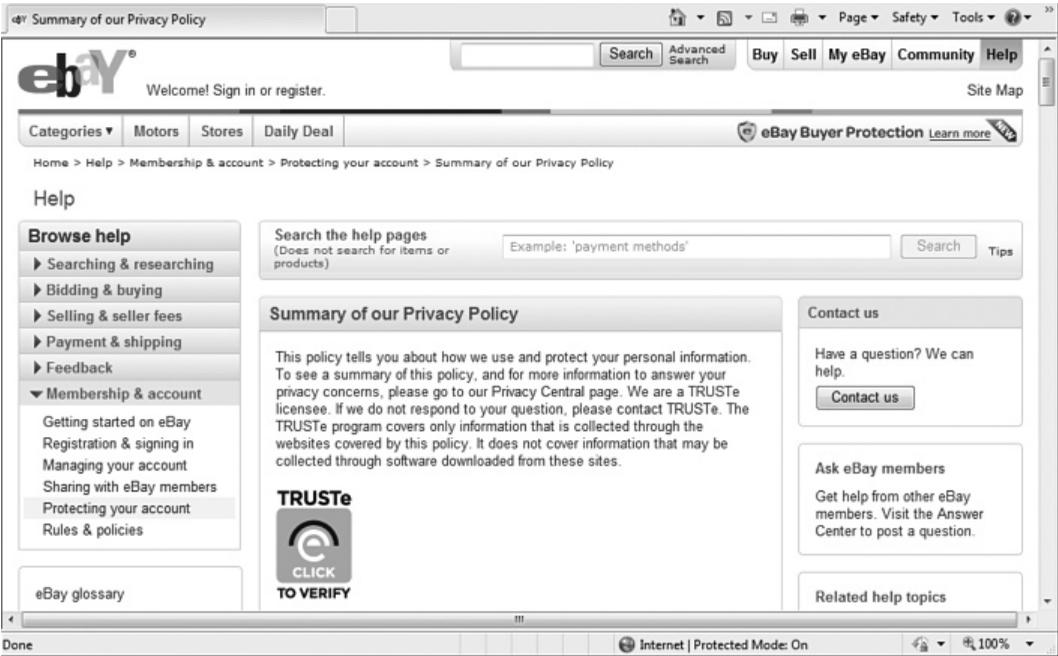
Where preference tracking becomes a problem is when you aren’t aware that your preferences are being tracked, or you’re not told who that data is being sold to or even that it is being sold. If you are aware that your online purchases are being tracked, remember to ask yourself, “How secure are the systems that keep track of what I buy?”

Most importantly, when you're considering a purchase with a new online site, find out what kind of privacy policies they have. Legitimate sites have links from the home page (and most other pages), taking you directly to the privacy policy.



The Amazon Privacy Notice link appears at the bottom of every Amazon page

That policy will tell you whether or not they sell information about you and your purchases. Don't assume that if the Privacy Policy is front and center that your privacy is being protected. A very large number of eCommerce sites DO sell information. They get away with that because most users never bother to read the posted Privacy Policy. Don't stay in the dark about where your information is going. Always read the Privacy Policy. No privacy policy? Then there's probably no privacy either. We strongly suggest you shop elsewhere.



eBay Privacy Policy

8.2.2 Hijackers

Unlike being pharmed, which can be good or bad, being **hijacked** is always a bad thing. What a hijacker does is send you to a different site than you think you're going to. You might believe you're at eToys.com when you're really looking at a well-spoofed site and handing your parent's credit card numbers to some con artist in the Ukraine.

Hijacking Rerouting a user from the website they thought they were going to into a different (often spoofed) site without their knowledge.

Spoofing

Users can be tricked in several ways. You already know that fraudsters often spoof well-known sites by creating fake sites that look very much like the real site but exist at a different Internet address (URL). Attackers send email and post links to the spoofed site in the hopes that unsuspecting users will enter personal and financial information. We talked about this in *Chapter 7, Phishing for Dollars*. The problem is becoming more common as phishing schemes proliferate but is thankfully easy to avoid. Simply NEVER go to a site by clicking on a link provided in an unsolicited email. Instead, type the URL as you know it in the address bar of your web browser. Problem solved.

Usually. Sometimes, however, the problem isn't a phishing scheme email so much as a user with poor spelling or typing skills. They type in the URL address themselves; they just don't spell it correctly. Spoofers select URLs that reflect common misspellings of commercial website URLs. Thankfully, most Internet security packages now check for this type of re-routing as part of their standard fraud prevention. That's one more reason to make sure that you're using a quality Internet security package.

DNS Poisoning

The second way that users are hijacked is harder to avoid. It's called a **DNS poisoning**. DNS poisoning occurs when a hacker breaks into your local DNS server. The DNS server (spelled out Domain Name Service) is what translates the domain name you type into the correct numerical Internet address. You type in `www.google.com` and it takes you to the specific Internet address where Google

lives. This greatly simplifies using the Internet for you, since it's a lot easier to remember a named URL like `www.CNN.com` than it is to remember an Internet address like `192.123.0.0`.

DNS poisoning Compromising a domain name server to hijack users without even their web browsers catching on.

A compromised DNS server can wreak havoc on Internet users. If your DNS server is poisoned, you could actually type in the correct URL exactly the way it should be typed and still end up on some con artist's website. Even worse, your web browser would actually believe that you were on the legitimate site. There's no easy way to tell you've been hijacked.

While DNS poisoning is thankfully much less common than spoofing or computer viruses, it does happen. One German teenager managed to reroute traffic to the German eBay site, `eBay.de`. According to police spokesman Frank Federau, the boy wasn't even a computer expert. He told police he'd just stumbled across a website explaining the scam and thought he'd try it out "for fun." Given that he's since been charged with computer sabotage under German law, we can only hope he's reconsidered his idea of fun.

While it's harder to protect yourself from DNS poisoning than it is to avoid clicking on spoofed email links, it is still possible. You can minimize your chances of being victimized by limiting your eCommerce dealings to those sites having a valid digital certificate. We'll explain more about certificates in the next section, but for now just remember that the certificate should match the location you were trying to get to.

8.2.3 Online Fraud

Online fraud includes purchased goods that fail to materialize, phony checks and electronic checks that never clear, work at home scams that never produce income for anyone but the scammer, and offers of "free" gifts and sweepstakes prizes which the user can claim only after paying shipping or taxes. In these cases, the prizes either never materialize or turn out to be worth substantially less than the handling fees required to collect them.

There's also a whole category of scams referred to as Nigerian money offers. This is one of the longest running scams on the Internet, having started in the 1980s, and seems destined to continue almost in perpetuity. Anyone who's used the Net more than six or eight months has received at least several of these offers. This scam is SO common that at one point, the Financial Crimes Division of the Secret Service received nearly 100 phone calls a day about it.

LAGOS, NIGERIA.
ATTENTION: THE PRESIDENT/CEO

DEAR SIR,

CONFIDENTIAL BUSINESS PROPOSAL

HAVING CONSULTED WITH MY COLLEAGUES AND BASED ON THE INFORMATION GATHERED FROM THE NIGERIAN CHAMBERS OF COMMERCE AND INDUSTRY, I HAVE THE PRIVILEGE TO REQUEST FOR YOUR ASSISTANCE TO TRANSFER THE SUM OF \$47,500,000.00 (FORTY SEVEN MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS) INTO YOUR ACCOUNTS. THE ABOVE SUM RESULTED FROM AN OVER-INVOICED CONTRACT, EXECUTED COMMISSIONED AND PAID FOR ABOUT FIVE YEARS (5) AGO BY A FOREIGN CONTRACTOR. THIS ACTION WAS HOWEVER INTENTIONAL AND SINCE THEN THE FUND HAS BEEN IN A SUSPENSE ACCOUNT AT THE CENTRAL BANK OF NIGERIA APEX BANK.

WE ARE NOW READY TO TRANSFER THE FUND OVERSEAS AND THAT IS WHERE YOU COME IN. IT IS IMPORTANT TO INFORM YOU THAT AS CIVIL SERVANTS, WE ARE FORBIDDEN TO OPERATE A FOREIGN ACCOUNT; THAT IS WHY WE REQUIRE YOUR ASSISTANCE. THE TOTAL SUM WILL BE SHARED AS FOLLOWS: 70% FOR US, 25% FOR YOU AND 5% FOR LOCAL AND INTERNATIONAL EXPENSES INCIDENT TO THE TRANSFER.

THE TRANSFER IS RISK FREE ON BOTH SIDES. I AM AN ACCOUNTANT WITH THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). IF YOU FIND THIS PROPOSAL ACCEPTABLE, WE SHALL REQUIRE THE FOLLOWING DOCUMENTS:

- (A) YOUR BANKER'S NAME, TELEPHONE, ACCOUNT AND FAX NUMBERS.
- (B) YOUR PRIVATE TELEPHONE AND FAX NUMBERS -- FOR CONFIDENTIALITY AND EASY COMMUNICATION.
- (C) YOUR LETTER-HEADED PAPER STAMPED AND SIGNED.

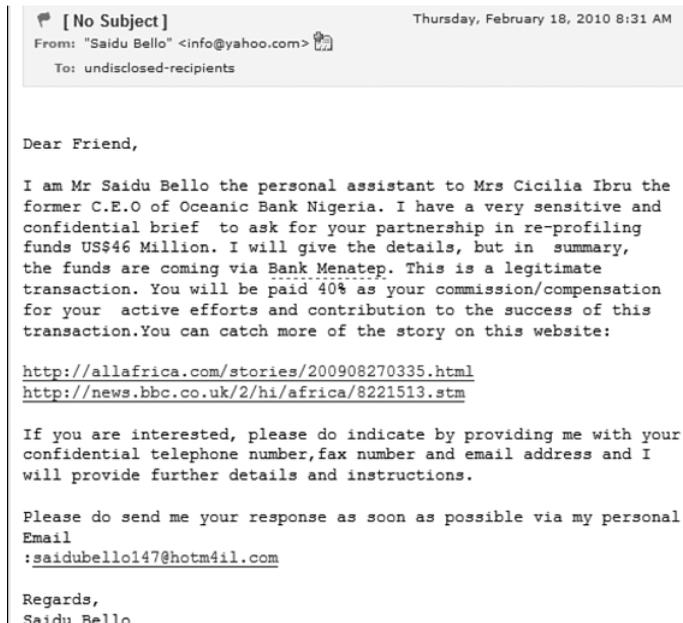
ALTERNATIVELY WE WILL FURNISH YOU WITH THE TEXT OF WHAT TO TYPE INTO YOUR LETTER-HEADED PAPER, ALONG WITH A BREAKDOWN EXPLAINING, COMPREHENSIVELY WHAT WE REQUIRE OF YOU. THE BUSINESS WILL TAKE US THIRTY (30) WORKING DAYS TO ACCOMPLISH.

PLEASE REPLY URGENTLY.
BEST REGARDS

Because this scam is so pervasive, there are probably several hundred variations on the theme. Some scammers throw everything into the subject, assuming that you're not likely to read the message body.



Others begin with the money scam approach, but are really angling to load your computer with malware by piquing your curiosity enough that you forget common sense and click on links embedded in the email for “more information.”



A few even acknowledge how well-known the scam is before launching into it. This is a great social engineering approach. The crook is basically saying, “Poor me. Wouldn’t it be awful to be a legitimate businessman in a country that’s known mostly for its online criminals?”

Still, our favorite would have to be the Nigerian scam that’s spoofed to appear as if it came from the FBI.



One of the best ways to keep your online purchasing experience pleasant is to limit your purchases to reputable sellers. Like many security measures, this is, of course, easier said than done. An easy first step, however, is to avoid buying anything from spammers. Nearly a quarter (24%) of Internet scams begin with unsolicited email.

Before you bite on one of those too-good-to-be-true email offers, you might want to consider the advice of Bob Kruger, a vice president at BSA. He notes, “There are a lot of cyber-grinches out there who are only too happy to take consumers’ money and spoil their holiday shopping season.”

8.3 Ensuring Safe Shopping

While computer fraud has advanced in recent years, so has the technology that can help to protect the integrity of your online communications and financial transactions. Three of these technologies are especially important: encryption, authentication (SSL, digital signatures, digital certificates), and security tokens.

8.3.1 Encryption

Encryption is a technique used to scramble content in files that you don't want anyone to be able to read. This protection is critical to safe online shopping. When you shop, you're sending a LOT of information that you really don't want to share with the general public. Your credit card numbers. All your personal information—your full name, address, phone number(s), and email address(es). Encryption of one or more forms is crucial to protecting all that shopping information.

When you encrypt a file, you're applying a “code” to it so that anyone who doesn't know the code can't read the file. Unscrambling an encrypted file so that it's readable again is called decrypting it.

You can think of **encryption** as applying a type of secret code. Remember the codes you used to have to break for math class to learn logic? “Decode the secret message if A=1, B=2, C=3, etc”? This is exactly like that.

Encryption Applying a secret code (cipher) to your messages or files to keep other people from reading them without your permission.

Let's use a simple code as an example. Let's say that we're going to encrypt a message by replacing every letter with the letter that precedes it in the alphabet. Every B becomes an A, every C becomes a B, etc. When you get to the beginning, you wrap around so that every A becomes a Z. Using this code, let's encrypt the following phrase:

This sentence is none of your business.

Once we apply our “cipher” (the alphabet precedence algorithm), this becomes:

Sghr rdmsdmbd hr mnmd ne xntq atrhmdrr.

In computer terms, the first sentence, the one you can clearly understand, is called **plaintext**. This is your text, plain as day, just the way you entered it from your keyboard. The scrambled sentence at the bottom is called the ciphertext. That's your text once the encryption cipher (sometimes called the cryptographic algorithm) has been applied. If you don't know the cipher being applied, it's very difficult to figure out what the second sentence means. So, it's extremely hard to decrypt the ciphertext.

Plaintext The plain, clearly readable, text message *before* encryption.

Of course, computer ciphers are an awful lot more complicated than our sample code. Most use at least a 64-bit encryption (often 128-bit). That means that the cipher key (that's a type of password that determines the cryptographic algorithm applied to encrypt your text) has at least 64 digits—possibly many more—that need to be puzzled out in the correct sequence for a code breaker to have any hope of decrypting your message without your permission.

In Internet security terms though, even 64-bit encryption is considered pretty simple—in fact, almost lame. Larger keys are used to produce stronger encryption. In general terms, encryption strength is measured by the encryption algorithm and the size of the key. A bigger key usually means stronger encryption.

Cryptoanalysis Trying to break an encrypted message.

In addition to encryption key size, encryption methods also vary. Today, there are two major methods used to encrypt communications over the Internet: symmetric encryption and public key encryption. Symmetric encryption, also called secret key encryption, uses the same key to encrypt and decrypt the message. In symmetric encryption, both the sender and the receiver have to have the same key. Therefore, the key must be kept secret. Public key encryption uses two keys: a public key and a private key. You can use either key to encrypt the message but only one of the keys will decrypt the message.



Ciphertext A message or file after it's been encrypted. Ciphertext appears garbled and can't be read until it's decrypted.

What all of these methods have in common is that you **MUST** have the cipher or key to translate the ciphertext back into plain text that makes sense. No key, no content.

As you might imagine, cryptography and the art of computer encryption is pretty complicated as well as just being pretty cool. If you'd like to learn more about this topic, we suggest you start by reading *Applied Cryptography* by Bruce Schneier.



8.3.2 Secure Socket Layer (SSL)

SSL is an important layer of security if you are providing personal information such as in a credit card transaction. SSL is a protocol that encrypts the transmission of data via HTTP. You can tell if you are protected by SSL if the browser

Common Codes and Dead Cows

Ciphers—secret codes—are pretty common on the Net. IM speak (R u hm for Are you home?) is one example of a common online cipher.

Another popular code is called 1337 (and pronounced “leet”), named for the 1337 (numerical) port used for an infamous computer attack by the hacker group that calls itself the Cult of the Dead Cow.

In 1337, words are spelled using numbers and symbols to replace the letters that they physically resemble. A simple example would be:

31337 h4x0rz un j00! > Elite hackers own you!

Fluent 1337 sp33k3rz get even more obscure, replacing R's with “/2”, etc. and making some pretty wild substitutes for other letters such as M, N, and W:

_|00 |2 4/\ / ()83|2 | -|4><0|2! > You are an uber hacker!

Also note that while many 1337 comments are insults (something about the gaming culture?), you can also use 1337 to send hugs and kisses, ><><<000><><<000, and love, <3 !

address bar displays an “https” instead of “http”, and if you see the lock symbol on the bottom right of your Web browser status bar.

8.3.3 Digital Signatures, Certificates, and Hashing

While encryption protects the contents of your message, it does nothing to prove or verify that you’re the person who actually sent it. This process of proving the source of a message or website is called **authentication**.

When you’re shopping online, authentication is a pretty important concept. Before you hand over your parents’ credit cards numbers to iTunes to download your favorite group’s latest album, you want to make sure that it really is iTunes that you’re talking to. In that case, while you still want and need to have those credit card numbers encrypted, you also want and need to authenticate the recipient.

Authentication Verifying the identity of a message sender or website.

Who Provides What?

Legitimate retailers know you’re concerned about potential fraud. So, they provide things like digital signatures and certificates to prove to you that they’re who they say they are. You just make note of what the vendor is doing to protect your data. You don’t actually have to DO anything.

Three common methods are used for authentication: hashing, digital signatures, and digital certificates.

Hashing

Hashing, most commonly a one-way hash, is a method used to verify data rather than encrypt it. With this method, a one-way hash algorithm is applied to the plaintext. The result is a “message digest” attached to the original plaintext message. This digest functions as a unique, identifiable “fingerprint” for the message.

If the message is changed in any way, applying the one-way algorithm will generate a “fingerprint” that no longer matches the attached digest. This process allows the message recipient to check the plaintext message received against the message digest to ensure that the file was not tampered with.

Digital Signatures

A digital signature is another method used to verify the sender of a message. Unlike hashing, digital signatures do use encryption—specifically, a type of public key encryption which uses two algorithms, one for encrypting and the other for decrypting the digital signature.

In simple terms, a digital signature is attached to encrypted data to ensure two things: (1) that the message is authentic and intact and (2) to authenticate the message sender. Using a digital signature has the same effect as using hashing along with encryption. It simply does so using a slightly different methodology.

Digital Certificates

A digital certificate takes the digital signature concept to a higher and much more secure level, by adding a trusted third party. When you buy something over the Internet, for example from Amazon.com, you are using public key infrastructure. The problem with using only public key encryption in this case is that anyone can create a public/private key pair. It's a bit complicated, but the basic idea is that it is possible to “forge” a digital signature. The signature itself would still match (the public/private key combination would still work), but the signature author might not be who you thought it was.

To avoid the problem of forged digital signatures, eCommerce retailers instead make use of a digital certificate. A digital certificate contains a person's or corporation's public key. This is exactly like a digital signature. The difference is that a digital certificate is issued by a trusted third party who verifies independently that the certificate belongs to the person claiming ownership.

You can think of a digital certificate as being analogous to a driver's license. When you obtain a driver's license, you have to provide reasonable identification to the Department of Motor Vehicles (DMV). The companies that issue digital certificates, like VeriSign, function as the DMV and obtain that reasonable identification. VeriSign's certification authority (CA) then issues a public/private key pair (for a small fee), keeps the matching public key in a database, issues a digital certificate, and keeps a copy of the certificate in its database.

8.3.4 Security Tokens

Encryption protects the contents of your messages and files. Hashing, digital signatures, and digital certificates authenticate the people and places that you're doing business with. **Security tokens** authenticate YOU.

You're probably thinking, "But I do that myself when I enter my private password." True. The problem is that passwords can be easily cracked and stolen by hackers. Security tokens provide a much stronger two-factor authentication that includes both data (often a password) and a physical device.

Two-factor authentication is something that you already use all the time offline. When you use an ATM card to withdraw money from your bank account, you're using two-factor authentication. The physical ATM card identifies you (factor one), as does the PIN number that you enter (factor two). While it's important that you don't misplace either, neither is really useful without the other. A criminal can play with your ATM card all day, but he's not getting money from your bank unless he also knows your PIN number.

Security token A two-factor authentication method using a physical device as well as a secret code.

An ATM card is only one example of a security token. Other forms of security tokens are physical tokens (a small hardware device), smart cards, and biometric systems. With biometrics, the physical component is biological data like a fingerprint or retinal scan.

OWN YOUR SPACE

KEEP YOURSELF AND
YOUR STUFF SAFE ONLINE

THE BOOK FOR TEENS THAT EVERY PARENT SHOULD READ!

A collaborative project to provide free security learning to teens and families online, made available under the Creative Commons Licensing, and made possible by the support of individual and corporate sponsors.

Every day, millions of American school children log on or log in and make decisions that can compromise their safety, security, and privacy. We've all heard the horror stories of stolen identities, cyber stalking, and perverts on the Internet. Kids need to know how to stay safe online and how to use the Internet in ways that won't jeopardize their privacy or damage their reputations for years to come.

Learn how to

- Kill viruses, worms, Trojans, and spyware
- Deal with cyberbullies
- Give SPAM the curb and smash web bugs
- Understand just how public your "private" blogs are
- Keep wireless freeloaders off your network
- Prevent sexting from ruining your life

About the team

Linda McCarthy, the former Senior Director of Internet Safety at Symantec, wrote the first edition of *Own Your Space*. With 20+ years experience in the industry, Linda has been hired to test security on corporate networks around the world. For the 2010 edition, Linda's expertise is backed up by a full team to provide the best security experience possible for teens and families online. That team includes security experts, design experts, anime artists, and parent reviewers, as well as a dedicated group of teen reviewers, web designers, and test readers.

General Computing

ISBN 978-0-615-37366-9
5 1 9 9 9 >



9 780615 373669

\$19.99 US / \$24.99 CAN

Cover design: Alan Clements
Cover artist: Nina Matsumoto
Cover illustration © 100pagepress

www.100pagepress.com



 page press

Smart Books for Smart People®