PayPal™ | Press

The PayPal Official Insider Guide to INTERNET SECURITY

Spot scams and protect your online business

Michelle Savage

The PayPal Official Insider Guide to INTERNET SECURITY

Spot scams and protect your online business

Michelle Savage

PayPal™ | Press

The PayPal Official Insider Guide to Internet Security

Michelle Savage

This PayPal Press book is published by Peachpit.

For information on PayPal Press books, contact:

Peachpit
www.peachpit.com

To report errors, please send a note to errata@peachpit.com

Project Editor: Michael J. Nolan
Development Editor: Matthew T. Jones
PayPal Press Managing Editors: Karen Richards and Jonah Otis
Production Editor: David Van Ness
Copyeditor: Gretchen Dykstra
Proofreader: Jan Seymour
Cover and Interior Designer: Charlene Charles-Will
Compositor: Myrna Vladic

Notice of Rights

Notice of Liability

The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor Peachpit shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the computer software and hardware products described in it.

While every effort has been made to ensure accuracy at the time of writing, the products and offerings by PayPal, including pricing and the manner in which they are accessed or controlled through www.paypal.com, are subject to change without notice. Subjective statements about the quality of products described in this book are not claims by PayPal but represent the sole opinion of the author.

Trademarks

ISBN 13: 978-0-133-15461-0
ISBN 10: 0-133-15461-0

To my amazing parents, Mary and John Savage,
who taught me the importance of feeling secure.
They've been my safety net my entire life.

Michelle Savage is a creative, professional writer, who has written books, articles, Web content, marketing materials, and educational guides for various corporations and publications, including PayPal, eBay, Microsoft, Symantec, TrustedID, SBC, Suze Orman, and Yahoo. Born and raised in New York City, she moved to the San Francisco Bay Area during the dot-com boom in the late 1990s. Since then, she has specialized in Web writing and digital media, focusing on online security, mobile security, social networking, and privacy protection topics.

Acknowledgments

Author's Acknowledgements

I would like to express my deep gratitude to the many people who saw me through this book; to all the experts who provided support, took the time to explain complex concepts, read, wrote, offered feedback, allowed me to quote them, and assisted in the editing, proofreading and design.

I would like to thank my PayPal Press and PeachPit Press for enabling me to publish this book. Above all I want to thank my husband, Josh, and my daughters, Camryn and Taylor, for giving me the support I needed, despite the amount of time it took me away from them.

I would like to thank Matt Jones, my editor and mentor at PayPal, who made a phenomenal contribution to this book, and Eunice Louie, Cynthia Robinson, Jonah Otis, Karen Richards, Marcus Meazzo, Markus Jacobsson, Bill Leddy and Gus Maldanado for their vision and support.

Last and not least: I would like to thank PeachPit Press's incredible editorial team for their incredible editorial contributions.

PayPal Press Acknowledgements

We applaud our PayPal security subject-matter experts whose knowledge was matched only by their dedication; Production Editor Karen Richards, whose diligent teamwork mastered our ambitious schedule; and Illustrator Gokul Nair, whose astute artwork enhanced the value of this book.

We'd also like to thank the following PayPal Press executive content and design sponsors for their highly supportive and creative contributions: Janet Isadore, Jonah Otis, and Marcus Meazzo.

Foreword

Technology moves fast. So do criminals. Beleaguered online merchants might feel like the only thing more daunting than preparing for Web 4.0 is bracing for Malware 5.0. Cyber attacks hit large and small merchants alike, phishers and fraudsters seem to be everywhere, and identity theft is so prevalent that we know credit score jingles better than Top 40 hits.

But this is not the end of the world, and you can't afford to hide in the closet. Your customers are online, on their smartphones, and buying goods and services in a virtual market that's growing at an amazing rate. You've got to ride this digital wave, but also make sure you don't get wiped out by the bad guys.

Wait, you say. Isn't security what *you* do, PayPal? Why do I have to worry about this stuff? And you're half right. We have a small army of very talented people fighting cybercrime, protecting our customers' data, and shutting down scammers day and night.

But we need your help.

It's up to you to choose strong passwords, install virus software on your computers, educate employees about phishing emails, and safeguard your customers' personal information.

That's why we wrote this book: to be your partner in anticrime, to share what we know about protecting your business and customers, and to help you grow and thrive. Let's get to it.

—Russell Bauder
Risk Design Team Lead

Contents

This page intentionally left blank

4

Taking Care of Malware

One of the biggest safety misconceptions among consumers and online merchants is that their computer software assures effective Internet security; however, malware is a persistent problem for all concerned.

In this chapter, we'll explain the ways consumers' and merchants' computers are at risk of becoming infected by malware, including so-called viruses, worms, Trojans, zombies, spyware, and more.

We'll also identify unique malware security challenges and solutions for online merchants to help protect their computers, networks, and customer data.

What Is Malware?

Even though obvious effects of successful malware attacks on businesses—including gross fraud incidents and major data breaches—have become common, online merchants don't always fully understand or respond aptly to malware threats.

All types of malware (short for malicious software), such as viruses, worms, Trojans, and spyware, are written to harm or exploit computers and networks, either as acts of mere malice, or, more often and of greater concern, to steal personal and financial information for criminal gain.

While malware targets everyone who visits the Internet or uses a computer, it poses a unique threat to online merchants, whose websites are often vulnerable in more ways than their owners realize. Cybercriminals are on the lookout for such weaknesses, viewing unsecured data as an open invitation to scam and deprive legitimate businesses, especially new online merchants.

FAST FACT: With 2.1 billion people actively using the Internet, according to Pingdom, Web users account for 30 percent of the planet's population. Security experts estimate that hundreds of millions of malware-infected computers are roaming the Internet, too, looking for vulnerabilities in computers or exploiting malicious URLs. Between one-quarter and one-third of all home computer systems are already infected with some type of malware.

Cybercriminals use special malware to victimize others in varying degrees, ranging from minor annoyances (such as pop-up ads in a browser) to major financial losses (such as fraud committed using stolen credit card or banking details).

FAST FACT: In its annual Threat Report, the security software company Symantec said that it stopped 5.5 billion malicious attacks in 2011, even as cyberattacks grew 81 percent in 2011, with up to 1.1 million personal identities stolen via malware.

Why Online Merchants Are Tempting Targets

For years, banks and financial services firms topped the list of industries most frequently targeted in online attacks. As a result of bad publicity, high-profile data breaches, and stricter government regulations, most banks have since tightened their security policies and procedures, making it harder for scammers to steal customer information.

Online merchants are now among the most exposed industries for scammers to steal information from and commit fraud against. Let's look at the top three reasons why cybercriminals attack merchants:

1. **Online merchants have data that turns a profit**. Cybercriminals know that they can get much of the same information from an online merchant that they'd find at a typical bank, including customer names, addresses, credit card numbers, and bank account details. A clever scammer can use this data to commit identity theft or other types of fraud, or even sell the info on the data black market to big cybercrime rings.

2. **Scammers use many programming languages.** Cybercriminals know the security shortcuts that online businesses, especially small ones, take to save time and money setting up and maintaining a commercial website. As a result, the crooks know how to exploit vulnerabilities in the code.

3. **Scammers know many online businesses are lean organizations**. Those who work for a small company often have multiple roles. When an online company's marketing intern is also in charge of patching servers and updating browsers, some tasks may not be done properly. Unfortunately, mistakes in this area can be costly. Many online retailers running transaction servers don't have a formal way to patch software on their servers, and today's cybercriminals and malware authors are experts in exploiting the vulnerability of unpatched servers.

Without strong security software, solid policies, and best practices for online security, Internet merchants—large or small—are in danger of being attacked by one (or more) of seemingly endless strains of damaging malware.

PayPal INSIDER

Using Fraud Management Filters

If you use one of PayPal's payment processing products, you're protected by multiple fraud management filters. These are tools that can identify payment characteristics that may indicate fraudulent activity.

Fraud Filter Options

If a transaction is flagged by one of these filters, you then have the option of denying payments that are likely to result in fraudulent transactions, or accepting payments that are not typically a problem. You can even opt to further investigate flagged transactions, by comparing prior orders, for example, or by contacting the customer for more information.

Who Can Use the Filters?

PayPal provides free filters for all business accounts. These basic filters screen for the country of origin, the value of the transaction, and other criteria, thus protecting you from obvious fraudulent activity.

When you subscribe to PayPal's Payments Pro service (at an additional charge), you have access to more advanced filters. These filters screen for credit card and address information, lists of high-risk indicators, and additional transaction characteristics.

What Are the Benefits of Using the Filters?

You save valuable time by letting PayPal review transactions instead of doing it yourself. You also save money by identifying and stopping potentially risky transactions; this reduces chargebacks and lowers your cost of doing business. In addition, you typically end up with more accepted payments because PayPal applies your rules evenly, and with greater accuracy; good customers are less likely to be rejected in error.

Types of Malware

Before malware became such a present menace, viruses were considered the biggest threat to computer systems. In fact, many people still falsely consider antivirus software sufficient catchall protection for all types of malware.

While computer viruses are still a major problem, many types of malware have surpassed viruses in variety and threat level. Today's most malicious software can self-replicate and harm your computer without your knowledge or permission.

Knowing the most common types of malware—those notorious worms, bots, zombies, and spyware villains—will help you understand and avoid these attacks on your computer and your business.

Killer Worms

Computer worms are one of the most destructive types of malware, as they hide in your computer, probing for other computers on your network to infect.

A worm might infect a computer without any action from you, or it might trick you into opening a link from a Web page to infect your computer. And worms can reproduce fast, replicating as many as 250,000 times in a typical eight-hour workday.

A worm's capabilities and targets depend on the payload it carries. The payload is the part of malware written to execute a specific task (another part of the code is written to enable its replication).

Payloads can be written to delete files on an infected computer, launch a viral attack, disrupt network traffic, and attack email and social networks for various aims. For example, worms are often used to disrupt network services or create denial of service (DoS) attacks against businesses.

Tricky Trojans

Much like the infamous wooden horse that ancient Greeks used to deceptively enter and destroy the city of Troy, today's Trojan malware appears to be legitimate but can infiltrate and damage a computer. Victims are tricked into downloading and running the bogus software on their computer systems.

Once installed, a Trojan starts attacking its host computer and may strike by displaying annoying pop-up windows, spreading stubborn viruses, stealing personal data or passwords, or deleting programs and files.

Unlike computer viruses and worms, Trojans don't spread on their own by infecting other files or by self-replication. Instead, they engage unsuspecting users to create computer damage themselves by opening an email attachment or downloading a file from a website offering interesting games, quizzes, or software.

Such seemingly innocent actions can wreak havoc if you allow Trojans to access your computer. Some may even uninstall files, opening up a back door to your security system. In this way, Trojans can allow an outside user remote control of your computer to copy and resend confidential information.

Panda Labs, Panda Security's anti-malware laboratory, reports that in the first quarter of 2012, six million new malware samples were created, and Trojans now represent 80 percent of all new malware. As you can see in **Figure 4.1**, no other malware comes close, as even worms comprise just 9 percent of total malware.

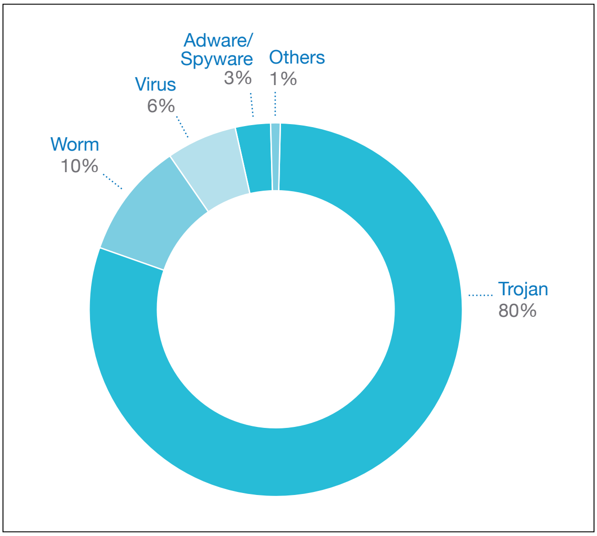

Figure 4.1 *Wondering what malware to combat most? Trojans account for 80 percent of all malware attacks.*

Source: Pandasecurity.com

Bad, Bad Bots

A “bot,” short for robot, is advanced malware that poses a major threat to almost any computer or mobile device.

Bots give cybercriminals major control over their victims’ computers. Bots use infected computers, known as “zombies,” to send spam, host phishing websites, execute DoS attacks, or steal victims’ identities by monitoring keystrokes.

A collection of bots in a network, or a botnet, can be deployed by organized cybercrime bot-masters to sell bots for malicious and illegal purposes. Bots have contributed in recent years to much corporate spying, government surveillance, and distributed denial of service (DDoS) attacks, which can shut down computer networks by accessing servers repeatedly and preventing legitimate customers from accessing websites.

Security experts say that there are thousands of bots and zombies on the Internet, and many may operate unnoticed for months as unwary computer owners endure their computers slowing down, showing strange messages, or crashing.

Prying Spyware

Fighting viruses, worms, Trojans, bots, and zombies has become a requirement for most businesses, and online security vendors have their protection down to a science.

However, another newer malware is using increasingly clever and sophisticated ways to sneak onto vulnerable computers: spyware.

Spyware is malware that gathers information from your computer without your knowledge and gives it to another party. Some irritating yet fairly harmless types of spyware may steal a computer’s power and memory, causing it to run slowly or even crash.

However, more dangerous spyware can steal your personal and financial data, such as your home address, email address, account passwords, credit card numbers, and more. And online merchants beware: scammers using spyware can get even more critical and useful data (for criminal purposes) about hundreds or thousands of your customers.

What Websites Are Most at Risk?

Certain websites—often for their size, prosperity, status, or popularity—are conspicuous and consistent targets of malware threats. Obviously, none of the affected businesses intends to cower or fold up in the face of malware threats—indeed, most are among the most highly protected and vigilant.

But all website owners are smart to understand which Web categories are most at risk, especially if their business depends on maintaining sound defenses against persistent cybersecurity attacks.

Security firm Symantec's 2011 Internet Security Threat Report lists the types of websites most frequently attacked and infested by various kinds of malware (**Table 4.1**):

Table 4.1

Most Exploited Websites	Percent of Infected Websites
Blogs/Web communications	19.8%
Hosting/Personal hosting websites	15.6%
Business/Economy	10.0%
Shopping	7.7%
Education/Reference	6.9%
Technology, Computer, and Internet	6.9%
Entertainment and Music	3.8%
Automotive	3.8%
Health and Medicine	2.7%

Furthermore, according to a 2011 Ponemon study, the rise of mobile workers, PC vulnerabilities, and the use of third-party applications on the network are the greatest areas of endpoint security risk today.

To prevent malware attacks, consider limiting network access via smartphones or personal devices, so that only certain staff members can access your networks. Even then, you might want to put further restrictions on access so that they can reach only certain parts of your networks.

How Is Malware Spread?

Cybercriminals constantly devise innovative means to get malware onto your computer. Here are some of the most common ways that malware, including viruses, worms, Trojans, and spyware, can be spread:

- **Email**: Cybercriminals are notorious for including malicious attachments and links in emails that appear to come from friends, reputable organizations, or other trusted sources. Some malicious emails can even infect your computer from the email client's preview pane, without your opening or downloading an attachment or a link.
- **The Internet:** Surfing the Web may feel like a private activity, but in fact you're exposing your computer to unwanted contact with anyone else who has a computer and Internet access. All you have to do is visit a website or click a link and you're a potential victim.
- **Outdated software:** Malware crawls the Internet, looking for vulnerabilities of outmoded software to spread its influence over computer systems. Be especially careful if you're surfing the Web with outdated software (and update with the latest versions as soon as you can), including your browsers, operating systems, or system plug-ins.
- **Local Area Networks (LANs):** A LAN is a group of locally connected computers that can share information over a private network. If one computer becomes infected with malware, all other computers in the LAN may quickly become infected as well.
- **Instant messaging (IM) and peer-to-peer (P2P) file-sharing systems:** If you're using a client for these online activities, malware may spread to your computer.
- **Social networks:** Malware authors take advantage of many popular social networks, infecting the massive user-data networks with worms. If a social website account is infected with a worm, just about anyone who visits a poster's profile page could "catch" the worm on her system.
- **Pop-ups:** Some of the most sophisticated malware spreads through well-disguised screen pop-ups that look like genuine alerts or messages. One particularly devious—and widespread—"hoax pop-up"

claims to have scanned your computer and detected malware. If you attempt to remove the malware as urged, you'll actually *install* the malware.

- **Computer storage media:** Malware can be easily spread if you share computer storage media with others, such as USB drives, DVDs, and CDs. While it may seem safe to open a CD of photos from a colleague, it's always best to scan unfamiliar files first for possible corruptions or security risks before you copy or open them.
- **Mobile devices:** Mobile malware threats have become increasingly prevalent (see Chapter 6, "INSERT CHAPTER TITLE"), as more people use their smartphones and tablets as mini-computers, helping malware problems proliferate across additional platforms.

Add Security to Gain More Trust

Some online businesses have no idea that they're infected with malware until they've been blacklisted by Google, which logs about 6,000 malware-infected websites every day, according to Business Week.

If a website is infected with malware and its name lands on the Google Blacklist, a merchant must prove that all traces of malware have been resolved before the name can be removed.

Here's how to remove a website name from the Blacklist:

- **Remove the malware.** Google suggests doing the following to fix the problem. Clean up the content, removing any pages that were added, any spam content, and any suspicious code identified by virus scanners or the Google Malware Details tool. If there are backups of the content, consider deleting the content entirely and replacing it with the last-known good backup (once it's clean and free of hacked content). Check to assure the hacked content is all gone by using the Fetch as Googlebot tool in the Google Webmaster Tools.
- **Change passwords**. Chances are, a merchant doesn't know how her website became infected and doesn't know what information the malware authors obtained. To be safe, change passwords so scammers can't access the website.

- **Request a review from Google**. When the malware problem is resolved, request that Google remove the website from the list. There's a link to request this review on the email Google sent noting that the website was blacklisted.

While it may be a surprise and a concern if your website gets blacklisted for security issues, the news should eventually better prepare your business to prevent malware attacks in the future.

Malware Threats Merchants Must Fight

Online merchants don't always have access to a team of security and network experts who can help them deal with cybercrime. While some are lucky to have a small IT staff or at least a consultant to answer their questions, many online merchants are mom-and-pop shops where it's actually *mom or pop* handling everything from customer service to protecting the security of their online operations.

Fortunately, there's outside help for one of the biggest concerns: fighting fraud when accepting payments online. A payment services provider like PayPal can help secure an online business (see the PayPal Insider in this chapter). Customer information is encrypted on the PayPal servers and any data that is passed between clients, retailers, and PayPal is secured using the latest safety technologies.

PayPal also encourages customers and online merchants to have a solid understanding of how malware works, how it infects computers, and how to spot signs of infection.

Here are some of the key malware risks you need to know about:

1. **Unpatched servers**: If you're using outside servers exposed to the Internet, or even internal servers that don't connect to the Internet, you're at risk for major security issues if you don't patch all your servers as soon as patches become available.
2. **Unpatched software**: Many free, mainstream Internet applications can contain security vulnerabilities to be exploited by worms or

viruses, and Internet security software vendors may take days or months to update their software to deal with new threats. In the meantime, your computer and networks are at risk. Fortunately, if you keep your browsing and email software updated with the latest security patches, you can minimize these risks.

3. **Insecure peer-to-peer (P2P) file sharing:** If you have file and printer sharing turned on, it's easy and convenient to share files with your coworkers. Individual users' computers often have file- and printer-sharing turned on, allowing files to be copied directly between computers within an office. While this is convenient and often essential to work group productivity, when it comes to confidential data, don't share these files unless they're stored on a secure server.

4. **Insecure passwords:** If you're sharing resources on a network, make sure they're password-protected. A strong password policy gives business owners control over who can access which resources, when they can access them, and what's available for sharing. Also, if an employee is terminated, it's easy to disable her network access.

5. **Personal laptops or mobile devices:** Both business-owned and personal laptops and mobile devices pose certain security risks to businesses. However, while business owners can control what a user does on company equipment, they don't have much say when it comes to what people do on their personal devices.

Security To-Do List

Malware isn't going away, so your best bet is to be well-prepared to deal with its potential attacks and aftereffects. As more people use the Internet to shop, bank, play games, socialize, and work, there are even more opportunities for cybercriminals to make a fast buck at others' expense.

Having read this chapter, you should be better able to spot and avoid different types of malware. Here are a few tips to remember as you read on:

- Implement a layered defense that includes firewalls, antivirus, and anti-spyware software, intrusion prevention systems, intrusion detection systems, and anti-phishing software.
- Keep systems and browsers updated with the latest patches. This helps prevent malware from infecting a computer, and also prevents existing malware from spreading across your networks.
- Monitor and quickly resolve any vulnerability that affects the programs and applications installed on your computer.
- When using social networks, be careful not to share too much information. If you're required to enter private data like an email address, select the option to prevent other users from seeing the information, to ensure that no one but you and the website administrator can access your data.
- Don't rely on a single operating system (OS) or browser. No OS or browser can be completely secure. By diversifying your OS and browser strategies, you ensure that your entire business won't be taken down by a single malware attack.
- Exercise caution when using smartphones, laptops, and mobile tablets to conduct business transactions. Being an online merchant is often a 24/7 job, which tempts some merchants to blur the lines between personal and business lives, and so expose their business data over unsecured personal-use mobile devices.

Next up in Chapter 5, "Steer Clear of the Social Engineer," we'll cover how to protect against major "social engineering" threats to your online business security.