Making Everything Easier!™

Symantec Website Security Special Edition

Website Threats

FOR DUMMIES®

A Wiley Brand

Learn:

- The potential cost to your business of an unprotected website
- The tools and tactics criminals use to attack your website
- How you can avoid the most common vulnerabilities
- How best to prepare for a possible attack

Brought to you by

Symantec™

The Symantec Team

Website Threats

FOR

DUMMIES®

A Wiley Brand

Symantec Website Security Special Edition

by The Symantec Team

FOR
DUMMIES®
A Wiley Brand

Website Threats For Dummies®, Symantec Website Security Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate
Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHOR HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS BOOK AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IT IS SOLD ON THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES AND NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. IF PROFESSIONAL ADVICE OR OTHER EXPERT ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL SHOULD BE SOUGHT.

ISBN 978-1-119-27539-8 (pbk); ISBN 978-1-119-27397-4 (ebk)

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@wiley.com.

Some of the people who helped bring this book to market include the following:

Project Manager and Development Editor: Chad R. Sievers

Executive Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Felicity Whyte

Dummies Marketing: Jennifer Webb

Production Editor: Vasanth Koilraj

Introduction

Welcome to *Website Threats For Dummies*, Symantec Special Edition, your guide to the different ways criminals can attack your website. This book can help you protect your website and, in turn, your business.

About This Book

Website threats are threats to your business. They aren't always easy to get your head around, so that's precisely why we wrote this book to be easily digestible.

Each chapter is self-contained, and you can pick and choose what you need to know.

You may think this book is going to be full of technical jargon and unfathomable geek-speak, but during the writing process, we have removed as much of that as possible and aim to explain everything in a language you can understand. Occasionally a bit of techy speak is necessary, but we always clearly define it, and it's pretty rare.

Keep this book on hand, and you'll know how to patch, protect, and prevent a serious attack on your business.

Foolish Assumptions

In writing this book, we make some assumptions about you. We assume the following:

- You're a business owner or you're responsible for a business website.
- You aren't especially techy, although you understand the basics. You're also short of time and like things explained in plain English.

- You have some basic knowledge about website technology. For example, you know terms like server, content management system, and browser.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

TIP

This icon highlights a particularly useful bit of information or way of protecting your website.

REMEMBER

You need to take note of these points. They're necessary rather than optional.

WARNING!

Warnings indicate information that could seriously affect your website or business. You need to pay careful attention when you see this.

TECHNICAL STUFF

This tells you that some techy speak is coming up. This information isn't essential to understanding the main point. If you skip this material, you won't miss out on anything that you need to know.

Where to Go from Here

To properly understand the threats your website faces, why they matter, and how to protect against them, then stick to tradition and start at Chapter 1 and go from there.

If you want to get straight down to technical details then you can leap in at Chapter 3 with tools of the attack trade and Chapter 4, which talks about what attackers can do with them.

There are specific tips throughout the book on how to stay safe, but if you want the bare essentials, then check out Chapters 5, 6, and 9.

Otherwise, just dip in for what you need. Whatever you do, this book can help you keep your website safe and in turn ensure your business isn't taken by surprise.

Chapter 1

Counting the Cost of Unprotected Websites

In This Chapter

- Calculating the financial costs of a compromised website
- Understanding the long-term impact after a breach
- Analyzing the risk a breach poses to your business

Imagine you're on a website, looking to buy a new pair of jeans or read a restaurant review. The homepage takes ages to load, and when it does, you find yourself being redirected to a different website while closing three unsolicited pop-up windows.

Would you buy something on this website? Would you trust it? Of course not. You'd click the back button faster than you can say "No thanks!"

Website security matters: research shows that approximately 70 percent of online shoppers cancel online orders because of trust issues. Consumers need to know a website is safe and that they can trust its owners with their personal information.

REMEMBER

Having an *unprotected website* — a website for which you haven't taken the necessary steps to defend it against the various threats outlined in this book — does more than put people off though. It exposes you to website threats that can cost your business a lot in lost revenue, operational costs, and fines. In fact, the Ponemon Institute's 2015 Global Cost of Data Breach Study estimates that a single data breach costs, on average, $3.79 million. That's $154 for every piece of data or information stolen from your business. And yes, we mean your business.

Small businesses are actually *more* likely to be the targets of costly attacks than medium-large enterprises according to the Symantec Website Security Threat Report 2016.

This chapter looks at the various costs — both financial and otherwise — to your business of a compromised website. Your website can be compromised in many ways, as we discuss throughout this book. With any kind of attack or breach, however, there are significant consequences for your business.

You face the immediate costs of dealing with the attack as well as reputational damage and the long-term impact of the incident. Treating website security as a business issue, rather than just a technical issue, is important, because the impact of a compromised website is certainly business-wide.

Adding Up the Immediate Costs of a Compromised Website

If your website is the target of a successful attack, even a relatively small-scale one, your business could be looking at reparation costs equal to the price of a fancy car, a yacht, or even an employee's annual salary.

These costs have a direct impact on your cash flow and inflict real-time damage on your business. The following sections discuss what you're putting on the line with an unprotected website.

Stolen money or data

Most cybercriminals are after one thing: money. They either want to steal it from you directly or steal data that they then can sell or use to access money that isn't theirs.

REMEMBER

Many types of data can be valuable to criminals, either to sell or use to set up fraudulent payments or identities. They might be after any of the following:

- Email addresses
- Financial details and credit card numbers

- Personally identifiable information that makes identity fraud easier
- Company secrets, financial details, or product specifications
- Passwords that gain them access to other parts of your business

An unprotected website gives hackers an opportunity to profit illegally, whether it's yours or your customers' money at stake, or even your customers' identity.

Fines

If your website becomes the target of an attack or data breach, you could face fines and legal penalties related to the loss of personally identifiable information (PII). Government bodies that regulate data protection can fine you, and customers seeking civil action can file a lawsuit against you to recover losses. Fines are based on a range of factors, including the size of the data breach and the extent to which your business failed to protect that data.

WARNING!

If you accept credit card payments on your website, you also have to comply with the Payment Card Industry Data Security Standard (PCI DSS), which strictly outlines your responsibilities around protecting customer data, such as names, addresses, and credit card numbers.

REMEMBER

Having an unsecured website means you aren't protecting your customers, as well as not complying with PCI DSS requirements. The fine for not protecting your customers' data can be as high as $1 million. You may also permanently lose the ability to process VISA and MasterCard credit cards if those companies, which help to create and monitor PCI DSS, find you don't comply with their standards.

Disruption to sales

When your website is down because of an attack, people can't access it. As a result, you lose customers and any revenue they would have brought with them because you can't sell your product or service to them.

According to the Incapsula Survey, "What DDoS Attacks Really Cost Businesses," businesses lose about $40,000 for every hour that a website is down. And the Ponemon 2015 Cost of Cybercrime Study found that cybercrime costs the average American firm $15.4 million per year, almost twice the global average. Ouch!

These numbers may sound large to a small business, but although the statistics may look less impressive when you hone in on just small businesses, the cost is actually much higher. According to the Federation of Small Businesses, a UK organization, cybercrime costs small businesses disproportionately more than big businesses.

In a 2016 report, the Federation found that, two-thirds of small firms have been a victim of cybercrime on average four times in the last two years, costing each business almost £3,000 in total.

Fortunately, investing in good website security costs a lot less.

Fixing the problem

How many analysts and IT specialists does it take to reboot a server, update configurations, and analyze logs? Sounds like the start of a joke, but the answer's definitely not funny.

If your website is breached or attacked, you need an IT team to fix it. And that means people, time, and a lot of money.

REMEMBER

Most small businesses don't have an IT expert on staff. Even when they do, that IT expert may not have the specific expertise to deal with a website attack. It's like having a doctor who's a general practitioner around when what you need is a cardiac surgeon who specializes in exactly the kind of treatment needed. Unfortunately, just like with that cardiac surgeon, hiring a specialist isn't cheap, especially when you need her immediately. The longer you leave an attack running, the more damage it can do.

In addition, you have to consider the personnel costs of handling customer complaints, public relations, and communications — time lost that employees could have spent doing their day job of sales, customer service, or product improvements.

How cheating on web security cost Ashley Madison billions

In 2015, controversial dating website Ashley Madison reported that its database, containing both member data and internal corporate data, had been stolen. Stored within the database was information on up to 39 million members including:

- Full names, usernames, and passwords
- Street addresses
- Dates of birth
- Partial credit card data and PayPal account details
- Phone numbers

What happened to all of this data? It was dumped on a website accessible only via an encrypted connection through an anonymous browser. It was also shared across the web, using BitTorrent. Thousands of people were revealed as having used the website, in addition to having their personally identifiable information (PII) exposed to hackers and identity thieves.

Luke Scanlon, a lawyer at Pinsent Masons, says that Ashley Madison could face costs of up to £1.2 billion in compensation in the UK alone — and that's a conservative estimate. Ashley Madison is already facing a $578 million class-action lawsuit, and founding CEO Noel Biderman has stepped down in the wake of the breach. The personal costs of the Ashley Madison breach are high for both company staff and website members alike.

Assessing the Long-Term Impact of a Compromised Website

Even if you manage to shut down an attack on your website, the costs don't stop there. The impact of a breach ripples out, racking up further costs and greater risks for your business. These sections examine the long-term effects, both costs and risks, that your business may suffer thanks to a breached website.

Brand and reputation

Putting a dollar value on your business's brand and reputation isn't easy, but you know that they're important and often worth a lot more than you think.

For reference, consider this: Apple's brand, according to Millward Brown, is worth $244.9 billion — more than the company's total revenue for 2015.

If you spent a lot of time building a name for your business, you don't want that name to become forever associated with a high-profile breach or lost customer credit card details. Similarly, your reputation is at stake: the trust that your clients have in your business. Without it, not only will clients shy away from recommending you to their peers, they may also actively spread negative opinions of your business.

REMEMBER

Ultimately, both things — brand and reputation — are about trust. And trust takes a lot of time and effort to build, but just a split second to destroy.

You may not be looking after a billion-dollar brand, but your brand and reputation matter all the same.

Personal cost

WARNING!

A data breach can put your personal reputation and job on the line too. As a business owner, executive, or IT professional, you're responsible for website security, and a breach that happens on your watch could spell resignation. For example, many high-profile data breaches in recent years have seen the dismissal of CEOs like Target's Gregg Steinhafel, who left the company after its historic data breach in 2014.

Traffic loss

Online traffic is essential to most businesses — whether your website is purely informational or an ecommerce website — it's all about visibility and popularity.

If you suffer an attack, not only will you lose traffic from wary customers avoiding the risk of landing on a questionable website, but your search engine rankings may also suffer a knock.

Google regularly crawls the web to identify and blacklist websites that appear to be hacked or involved in "suspicious activity."

If your website is breached or infected with malware, Google will issue a warning to your visitors. This might say something like "Something's not right here" or "This site may harm your computer," which isn't exactly good for business. It lowers your search engine ranking and results in fewer visitors and fewer customers, as well as you spending time and money, trying to get back into Google's good books.

Repairing the damage

When it comes to your IT, even after you've fixed the leak of a website breach, you still have to deal with all the water damage.

That means forensic investigations, legal costs, the costs of implementing new security measures, and much more. It can take months to uncover the full extent of a breach, and you never know what other risks and vulnerabilities will be discovered in the process.

You'll also likely have to invest in a cyberinsurance policy, which, although can help you offset costs incurred as a result of any future attacks, is likely to have higher premiums if you've already suffered an attack.

That said, it could be worth it if you're hit again; insurance can cover a range of expenses like forensic investigation, legal fees, and even potential lost revenue.

Relying on law enforcement is a mistake

Cybercrime is just that — a crime. And law enforcement agencies around the world work hard to track down, capture, and prosecute the criminals responsible for cyberattacks and data breaches. But they don't often succeed.

Enforcing the law when it comes to online crime is very difficult for several reasons:

- **Geography:** It's very common for a victim of cybercrime to be in a totally different country to the criminal carrying out the attack. Rules of jurisdiction mean it's hard to know who should be investigating a particular crime, and if the criminal is based elsewhere, quite often no authorities can arrest or extradite that criminal.
- **Complexity:** Laws that relate to online activity are both complex and very new, meaning there is little precedent in which to rely. Sometimes laws don't exist yet to ban certain activities online because up to now there has been no need to create them.
- **Difficulty:** The laws are difficult to understand. But even if a law enforcement agency is able to identify a crime and arrest a suspect, actually prosecuting them is equally difficult. "Prosecuting somebody for Internet-based credit card fraud is really, really complicated, and it takes a lot of time and effort," says Mark Surguy, Eversheds LLP Partner, specializing in fraud and financial crime.
- **Flimsy forensics:** To charge someone for a crime you need evidence. The problem with the evidence in a cyber crime is that it's ephemeral. As TechRepublic reports, "The problem with digital evidence is that, after all, it is actually just a collection of ones and zeros represented by magnetization, light pulses, radio signals, or other means. This type of information is fragile and can be easily lost or changed." Those investigating crimes can easily accidentally alter evidence, and many criminals set their programs to erase if they're detected anyway.

You can't, therefore, expect to get reparations for an attack. Claiming for damages is rarely an option, so stay safe and avoid attack in the first place.

Chapter 2

Getting to Know the Enemy

In This Chapter

- Identifying who poses a threat to your website
- Coming to grips with why people attack websites
- Understanding what people have to gain from attacking websites

You run a small or medium business and manage its website; everything seems fine. It doesn't seem likely that you're about to come under attack from cybercriminals, hacktivists, spies, and organized crime gangs, does it? You're not in some kind of futuristic mobster movie after all.

REMEMBER

But just because you can't see the criminals crashing through your shop door or rifling through your filing cabinet doesn't mean you aren't at risk. Don't be lulled into a false sense of security.

Many of the techniques that attackers use work on an industrial scale, utilizing the Internet's global reach and hijacked networks of devices, commonly computers, that criminals have installed malware on so that they can control them remotely without the owner knowing (known as *botnets,* which we discuss in Chapter 3) to attack any or all websites indiscriminately.

Plus there's the fact that, without the security resources of big companies, small- and medium-size businesses can struggle to meet the challenges of website security threats.

This chapter takes a closer look at the culprits behind website attacks. Understanding who is attacking your website and why they are attacking can help you strengthen your defenses and ramp up your emergency plan.

Criminals: Looking for Money

Criminals want money. They can use your website to install malware on your visitors' computers or, if they can shut down your website, they can demand a ransom. Criminals who attack your website come in two types: small-time and big-time. The following two sections examine them in greater depth.

Small-time crooks

Many websites are attacked at the hands of small-time crooks. Unfortunately, a person doesn't need much to start his own online criminal gang. If a criminal knows where to look, he can buy *attack kits* (software that lets someone hack into websites like we talk about in Chapter 3), custom malware, and even *denial of service attacks*, which we cover in Chapter 8, that allow a crook to shut down a website remotely.

Prices for these services start in the low hundreds of dollars on the black market. The rewards can be significant and, in some parts of the world, the risks of being caught are extremely low.

In addition, many individuals and small groups make a living contributing to the underground economy in other ways. For example, digital money mules use stolen credit cards to buy things that can be sold for cash. Malicious hackers write the malware and sell it to other people. They don't run the attacks themselves, but they're still supporting the criminals.

Big-time criminals

The big sharks are the most dangerous criminals. Organized crime, commercial spies, and even national spy agencies attack websites. They're persistent, crafty, well resourced, and in it for the long game and the big wins.

Why? The pickings are valuable. In 2015, for example, the White House, the Pentagon, the German Bundestag, and the US government came under attack while businesses saw hundreds of millions of identities stolen.

REMEMBER

As you've probably guessed, organized crime is in it for money and information, and they use these techniques to get it:

- **Protection rackets:** Shutting down websites while demanding ransoms to reopen them
- **Ransomware:** Illicitly encrypting a website's database or user information and demanding payment to send the decryption key
- **Data theft:** Stealing credit card information for fraud and personal information for identity theft
- **Scams and cons:** Redirecting people to gambling or porn websites to collect referral fees or getting people to visit a fake *phishing* (see Chapter 7 for more on phishing scams) website to pick up passwords
- **Installing malware:** Using website-installed viruses to take over your computer to send spam, launch attacks on other websites, or just steal your information

Done on a large scale, these activities can be very profitable. The revenue allows gangs to buy the latest software and zero-day exploits that make them more effective. It also lets them hire the smartest hackers and invest in research and development.

Cyberspies: Looking For Information

Espionage hackers often target smaller companies to get access to bigger firms that are higher up the supply chain. They want to steal corporate secrets, intellectual property, and information about employees.

It may sound like a bunch of nerdy James Bond wannabes but cyberespionage is real and dangerous. Government-sponsored cyberspies use sophisticated watering-hole attacks, where they break into websites that they know their victims are likely to visit in order to target specific visitors with specific malware.

For example, a spy agency interested in targeting central bank employees might hack a financial news website that the targets visit regularly. The agency might then use information collected in this way to infiltrate the bank to steal personnel records and gain access to computers and data on its network.

In recent years, nongovernment spies-for-hire have also arrived on the scene. For example, the Butterfly Group is a team of well-organized, highly capable hackers who use stolen secrets for insider trading on the stock market or sell it to the highest bidder.

Hacktivists: Spreading Their Message

Hacktivists attack companies and organizations they don't like, trying to disrupt their operations, vandalize or deface their websites, or stop people from visiting them. Hacktivists are people with a political or social message to convey. But instead of writing a blog or taking out an ad in the *New York Times,* they attack websites. For example, they deface target websites with their own messages or block access to make a point. They don't just target big companies but also connected businesses, such as suppliers.

One such group is Anonymous, which has launched attacks on politicians, religious organizations, political parties, and businesses in support of causes it holds dear. It launched distributed denial of service (DDoS) attacks against the VISA, MasterCard, and PayPal websites, for example, after those organizations stopped processing donations to WikiLeaks. This made the websites temporarily inaccessible to visitors, costing the parent companies significantly.

Troublemakers: Creating Mayhem

Some people just want to cause mayhem because they can. So-called *script kiddies* use off-the-shelf hacker tools to vandalize websites and then show off about it.

There are also people, shielded by the anonymity of the Internet, who stalk, harass, and troll people and businesses out of sheer malevolence. For example, a geek with a grudge or a teenager looking for laughs could bring down your website just as easily as a criminal gang.

The black market price list

Sometimes criminals steal bank details from your business or your customers for the simple reason of taking money from those accounts. Often though, they'll be looking to steal data in bulk that they can sell on the black market.

This kind of data is often traded on the *dark web* — an alternative world wide web that you can only access via the Tor network — making the websites and the people that use them virtually impossible to trace.

The following table, taken from Symantec's Internet Security Threat Report 2015, gives you an idea of how much the data you hold about your employees or customers is worth to a criminal or gang and why they would want to attack your website:

Item	***2014 Cost***	***Uses***
1,000 stolen email addresses	$0.50 to $10	Spam, phishing
Credit card details	$0.50 to $20	Fraudulent purchases
Scans of real passports	$1 to $2	Identity theft
Stolen gaming accounts	$10 to $15	Attaining valuable virtual items
Custom malware	$12 to $3500	Payment diversions, *Bitcoin* stealing
1,000 social network followers	$2 to $12	Generating viewer interest
Stolen cloud accounts	$7 to $8	Hosting a *command-and-control (C&C) server,* which allows you to issue commands to a botnet and receive reports back from the devices in the botnet
1 million verified email spam mail-outs	$70 to $150	Spam, phishing
Registered and activated Russian mobile phone SIM card	$100	Fraud

Chapter 3

Recognizing the Tools of the Attack Trade

In This Chapter

- Understanding how criminals power cyberattacks
- Getting to grips with the weapons cyberattackers use
- Realizing how your own employees can be used as a weapon

To a veteran cyberattacker, websites don't look like they do to you; instead they look like a list of lucrative vulnerabilities that are just waiting to be taken advantage of.

Cyberattackers are more sophisticated than they look on TV dramas. They have an armory of weapons at their disposal that they can use to crack a website's weak points.

In this chapter, we look at the tools of the attack trade because knowing how these weapons work is half the battle to defending against them.

Powering Attacks: Botnets

For many attack tactics, criminals don't just need tools; they need an army — an army of compromised Internet-connected devices to be specific.

Botnets are a tried-and-true tool for cybercriminals, giving them the machine power to hunt out vulnerable websites or weak links in computer systems and then exploit them with maximum force.

These sections examine more specifically what botnets are and how criminals use them to get what they want.

Defining a botnet

A *botnet* is a group of Internet-connected devices, traditionally computers, which attackers have infected with malware. This malware then allows them to control the devices remotely. The name relates to the software that criminals run on these infected devices, *bots*. Bots are simple computer programs that can run autonomously and automatically over the Internet and that carry out simple, repetitive tasks.

REMEMBER

Most of the time, the owners of these devices aren't aware that their system has been compromised because the malware runs silently in the background and doesn't affect the way they use their machines. This doesn't stop their computer power being put to work for malicious purposes though.

Botnets in the real world

Take for example the ZeroAccess botnet, which in 2013 had a population of around 1.9 million computers. Rather than all being controlled by one "master," the malware automatically checked for other infected devices in the same local network, and if there were any, used those local machines to send instructions to the "new recruit." Because there was no single command-and-control center, it was much harder for the authorities to take the botnet down.

Criminals used this botnet for various schemes, including Bitcoin mining and click fraud, where the criminals could generate income from referral schemes by generating fake clicks on adverts or websites.

Each infected device could generate 42 false clicks an hour. Not much when each click is only worth a penny, or less, but multiply that by 1.9 million and the criminal could have been making tens of millions of dollars a year.

Understanding how criminals use botnets

By combining the power of these networks of compromised devices, attackers can send mass emails containing malware, or even perform distributed denial of service (DDoS) attacks, as we cover in more detail in Chapter 8.

Scarier still, with the growing availability of botnets-for-hire, criminals don't even need to build their own botnets to power their attacks. They can simply buy them on the black market.

Botnets-for-hire were implicated in roughly 40 percent of all DDoS network-layer attacks in the second quarter of 2015, according to Incapsula's report on the Global DDoS Threat Landscape.

Using botnets is like throwing a party and hiring a crowd of guests to fill it for you.

Executing Attacks: Web Attack Toolkits

Criminals no longer need to be tech wizards to launch an attack. Just like you can create a website without being able to code, criminals can simply buy a ready-to-use web attack toolkit with all the coding done for them.

A quick visit to their local black market store and attackers can stock up on all the malicious code they want. For more specific attacks, criminals can even get malware made to order — now that's good service. A lot of these transactions take place on the *dark web,* where it's very difficult to track activity back to specific individuals and locations, making it ideal for criminals.

These kits don't just include malicious code though; they also include tools for finding vulnerabilities, testing for security software, and dropping the malicious code or software into the compromised website.

In these sections, you can discover how attack kits scan devices for weaknesses and deliver precisely the right kind of malware for the attacker to get what they want from the victim's device.

Getting the lay of the land

Before attackers even attempt to breach website security, they need to work out what vulnerabilities a website has. Lucky for them, readily available programs called *vulnerability scanners* do that automatically.

Designed to scan all kinds of devices, these programs can run reconnaissance missions on anything from your server to your smartphone, and — if a vulnerability exists — they'll find it.

On their own, these aren't malicious programs. Security and testing firms use exactly this kind of vulnerability scanner to help companies find vulnerabilities; the open-source Metasploit Framework is one such example.

Cyberattackers, however, can use these programs to find vulnerabilities, which tells them what type of exploit or malware to use, greatly increasing their chance of success.

Attacking with web attack toolkits

After your friendly neighborhood cybercriminal knows your website's vulnerabilities, he can execute his attack. The attacker simply purchases the toolkit he needs and uses it to customize, deploy, and automate widespread attacks.

Targeting Software's Achilles Heel: Zero-Day Exploits

Keeping your website software and applications updated helps you to avoid most vulnerabilities, as we talk about in Chapter 6. But, due to the complex nature of coding, most software has several vulnerabilities. These vulnerabilities can exist for a long time without anyone realizing they exist. Sometimes a vendor does spot them, but doesn't immediately patch them.

If criminals discover one of these vulnerabilities, however, they can tailor an exploit to take advantage of it and can cause a lot of damage. With no patch, any device using the targeted software is vulnerable to that specific zero-day exploit, creating a huge target for criminals (or anyone who wants to exploit them).

The following sections help you better understand what zero-day exploits are, including how attackers use them, and what you can do if your website is attacked.

Knowing the basics of zero-day exploits

Zero-day exploits are attacks that target software vulnerabilities discovered by attackers before the software provider has released a patch to fix them.

TECHNICAL STUFF

A *patch* is a software term that is a kind of update. When software developers notice a problem with their software or a security flaw in the coding, they can write new code to patch the flaw. Then, after they've tested it, they can release the patch for you to download and install.

If no patch is available — often because no one knows about the flaw — criminals have free rein to exploit the vulnerability at will. Some of the most serious zero-day exploits have allowed attackers to uncover private customer information, enraging the software's customers and embarrassing its developers.

Taking action when a zero-day exploit hits your website

In 2015, the number of zero-day vulnerabilities more than doubled from the previous year, with a new zero-day vulnerability being found every week on average, according to Symantec's 2016 Website Security Threat Report.

That's a lot of opportunity for new exploits, and, unfortunately, that makes it likely that one will hit your website.

If you're attacked, follow the instructions the software provider gives very carefully. You should also look to trusted security sources that publish information about the actions you can take to limit the damage to your business.

Going behind Enemy Lines: Disgruntled and Exploitable Employees

If attackers can't access your website from the outside, they may recruit the help of someone on the inside.

The colleagues that you trust most can easily give away passwords to your website, the server it's stored on, and the cryptographic material used to secure and facilitate an attack.

But why would trusted colleagues turn against their own website? There are plenty of motivators:

- The criminal who is looking to profit from the attack offers a lucrative payment to your employee.
- The employee wants to plot revenge after a problem in the workplace.
- The employee seeks to make money by working with the attacker to blackmail the website owner.

TIP

Make sure that you limit the number of people who have access to your website and its security features. If an employee changes roles or leaves your company, change the passwords and revoke her access.

The cyberattack market in action

On Christmas Day 2014, a group calling themselves The Lizard Squad claimed to be behind a DDoS attack that caused long-lasting outages to Microsoft's Xbox Live and Sony's PlayStation Network services.

The group said the whole attack was orchestrated to promote its new web attack toolkit — the Lizard Stresser Tool — so that the attackers might sell it to others who wished to carry out similar attacks. The tool, which brought the gaming services to a standstill, drew on the bandwidth of a botnet of worldwide home Internet routers.

Aside from fueling a huge number of complaints from angry gamers (you wouldn't like gamers when they're angry) and causing serious financial repercussions for the companies involved, the attack showed just how bold the cyber-attack industry has become. This attack was just one of many carried out using the tool, all courtesy of software sold as a service to budding cybercriminals.

Chapter 4

Understanding How Attackers Exploit Vulnerabilities on Your Site

In This Chapter

- Requesting information from your server with SQL injection
- Forcing their way in by cracking your passwords
- Attacking visitors using fake ads
- Installing malicious code to run on your website server

Imagine there is no Internet. Now imagine that criminals want to attack your business. They may break into your shop or office and steal money. They may deface your billboards or storefront. A rival may try to steal your customer details. Perhaps they demand protection money. They could even pretend to be you and steal from your customers and damage your reputation.

With the Internet, crooks can do all those things using your website.

In this chapter, we explain some of the ways Internet criminals attack particular vulnerabilities on unprotected websites.

These methods include the following:

- Breaking in to your website database through the forms on the website
- Hacking into the server that runs your website to gain control over the website
- Running fake ads on your website (if you have an ad-funded business) that contain malware

Forget the image of a lone wolf hacker in a dark room targeting individuals. As we discuss in Chapter 2, all types of criminals can attack your website. Oftentimes, criminal gangs run these attacks on an industrial scale and target anyone that has a vulnerability they can exploit. Being a small or relatively unknown business won't protect you.

Breaking Down the Front Door

One of the most common types of website attack is the *SQL injection attack,* which exploits weaknesses and bad programming in website software. This type of attack gives criminals the ability to extract, delete, or change data used by the website, such as customer records, content, and user names.

Criminals use bots to test for this vulnerability on thousands of websites at a time, hoping to find one that is unprotected and vulnerable. It's a bit like a car thief going down the street testing all the doors to see if any are unlocked. (Chapter 3 provides more discussion about bots and botnets.)

The consequences of an SQL attack can be huge. Experts think attackers used this technique to steal the personal details of four million customers from a UK phone company.

The following sections look at how SQL injection actually works and how to reduce the risk of your website falling victim to this type of attack.

Grasping how SQL works

Most modern websites use a database to store pages, images, and all the other bits and pieces that go together to make a webpage. These databases use a language called SQL (which stands for Structured Query Language) to communicate between the software that delivers the web pages and the database itself.

In other words, SQL is a way of saying "Hey, can you send over that picture of a pony and all the comments about it?"

The problem is that many websites have some kind of input form, such as a contact us page or a blog comment field or an order form. Those forms use SQL too, which means that a cybercriminal can put SQL code into the text fields of a form designed for humans and — on vulnerable websites — get the database software to run that code.

For example, a criminal could inject a request for the database to send a list of all the user names and passwords on the website. The database's response would simply appear in the criminal's browser like any other web page.

Reducing your vulnerability

You can take action to reduce the risk of falling victim to an SQL injection attack by ensuring the code used to build your website and the software running on it doesn't contain vulnerabilities that attackers can use to carry out SQL injection. You can also use form validation to make sure that any form entries are checked for the telltale signs of an attack before submitting them to the database.

Here are some actions you can take to decrease your risk:

- **Take a leaf out of the attacker's book and use a scanner on your website to test for vulnerable forms.** Just as there are virus scanners for your PC, there are vulnerability and malware scanners for your website, including pro tools like Metasploit, W3af, and Grabber. Use them to identify what you need to protect or repair.
- **Hire professional penetration testing firms to check your website for vulnerabilities.** Look for reputable, certified organizations to help you test your defenses. In the UK, the government's CESG has a Certified Cyber Security Consultancy program and similar schemes exist in other countries.

- **Make sure that your website software is up-to-date.** As software developers discover vulnerabilities in their applications, they fix them, but you don't get the benefit unless you install the update. Also consider using website software like WordPress, which automates security updates.
- **Take care with plug-ins and add-ons for your website to make sure they don't open a door you thought was locked.** Many popular website content management systems, such as WordPress and Joomla, allow website owners to add extra functionality using plug-ins. But every time you add one, you could be adding code to your website that is vulnerable. WordPress automates its security updates and most major plugins piggyback on that capability — just make sure you use plugins that do. More generally, look for add-ons that are regularly updated, widely used, and well supported. Where it's not automatic, make sure you update them regularly too.
- **Work with your developers.** For many websites, regular testing and updates is enough. The firms that make the software will do the heavy lifting of maintaining the code for you. However, some websites include custom code and unique features. If you have hired developers to build this kind of additional functionality for your website, have them check it regularly too to make sure it doesn't open a back door to SQL injection and other threats. Before hiring a website development company, make sure it understands the security risks (and maybe provide a copy of this book!).

Sneaking In through the Back Door

Some criminals work by kicking in the front door, trying lots of websites to see if SQL injection attacks might work. However, others sneak in through the back door by getting hold of passwords to access the servers and applications that run your website.

These sections explore ways to stop this happening, protect your systems from unauthorized entry, and choose stronger passwords.

Assessing the importance of passwords

Running a website takes a lot of software and hardware. There's a database server, a website server, content management systems, and more. The hardware side includes computers and network equipment. All of them have passwords. And if a hacker has your password, it's game over.

WARNING!

If a hacker knows your password, he can pretend to be you and do whatever you can do. For example, if a hacker has the password to your content management system, he can change the contents of your website, add new code, or even shut it down altogether.

Lowering your exposure

You can defend your website by strengthening and protecting your passwords. Unfortunately, weak passwords are commonplace. Some systems are even left with manufacturers' default passwords in place. Hackers know this and use libraries of common passwords and tools that try thousands of passwords a minute to attempt to gain access.

TIP

In order to keep your metaphorical back door locked, do the following:

- **Use stronger passwords.** A strong password is between 30 and 50 characters long. That sounds like a lot but you can manage your strong passwords in two simple ways:
  - Use a password manager, which randomly generates long, complex passwords and remembers them for you.
  - Use a long string of random (but memorable to you) words. Don't use well-known lyrics or phrases or information that's personal to you like addresses. Just use unconnected readable words that will stick in your mind, such as, "copy bright top goat swimming freely."

- **Limit the number of people who have access to website servers and content management systems.** Decide who you trust to have access to your systems based on their job duties, experience, and training. Make sure they don't share passwords. Delete their access and change passwords when one of them leaves.
- **Change your passwords on a regular basis.** Changing passwords regularly is good practice — anywhere from once a month to once a year, depending on the sensitivity of the system in question. Doing so reinforces the company password policy and also reduces the risk that an undetected hack or leak leaves you vulnerable.
- **Use two-factor authentication (2FA).** You need two different components to verify your identity. These components can be something you have, something you know, or something inseparable from you, like a fingerprint. A common example of 2FA is when you get money out of an ATM; you need both the physical card that you have and your PIN that you know.

Spreading Malware Via Fake Ads

Many websites make money by selling advertising. The problem is that as ads become more interactive and sophisticated, criminals can embed malware into them and get them placed on innocent websites. The danger for you as a website owner is that you end up infecting your customers and visitors unwittingly, which isn't a good way to win friends. Worse, if your website is infected with *malvertising,* Google could blacklist you and your website could trigger warnings on your visitors' computers. The result? Your traffic plummets.

The following sections look at how malvertising works and what you can do to try and avoid working with an ad agency that unwittingly posts malicious ads on your website.

Grasping how malvertising works

For criminals, *malvertising* — malicious or malware-infected advertising — is a smart and ruthless way to get their malware onto people's computers. They buy advertising on legitimate websites through legitimate ad brokers and embed malicious code in those ads that installs malware on vulnerable computers when people see the ad.

If a website visitor is exposed to one of these ads and gets infected, he could be vulnerable to identity theft, computer problems, *ransomware* (malware that encrypts files on your computer so you can't open them anymore or locks your whole device and then demands a ransom fee, which may or may not actually unlock the files or device), and other risks. And all he did was visit your website.

Diminishing your risk

To reduce your risk of being a victim to malvertising, make sure you do the following:

- **Choose reputable advertising brokers and partners.** Ask whether your advertising firm checks for malware and takes other measures to block malvertising. Choose well-known companies rather than unknown agencies that might be more vulnerable.
- **Keep an eye on Google Search Console (the tool formerly known as Google Webmaster Tools).** Doing so can help you ensure that you're in good standing with the superstar of search engines. If Google detects malware on your website, including malvertising, it hides your search results. If you don't use Google Search Console, you may not know that this is happening until you see your organic traffic plummeting.

Lying In Wait with Malicious Code

Webpages stopped being static pages of text and pictures in the '90s. Today, website developers use programming languages like JavaScript to add interactivity to a webpage.

The problem is that if criminals gain access to your website, they can also add their own code to your website, which runs when people visit it. This type of assault is referred to as a *cross-site scripting (XSS)* attack.

The following sections explain how XSS works and what it can do, or allow attackers to do with your website. You can also read about ways to prevent criminals from being able to carry out a XSS attack on your website.

Comprehending how an XSS attack works

In a cross-site scripting (XSS) attack, criminals try to find a vulnerability in the software that runs your website so they can piggyback their own code on your pages.

Malicious JavaScript, for example, can use information in the browser to pretend to be your visitors on another website. Or it can access a visitor's webcam or microphone, or display unwanted advertising and direct visitors to phishing websites.

In some cases, sophisticated hackers can use cross-site scripting and other forms of attack to install hard-to-detect spyware on website visitors' devices.

Reducing the threat

You can take action to reduce the risk of falling victim to an XSS attack by following these steps:

- ✓ **Run regular scans on your website for vulnerabilities and infections.** You can scan your website for problems just like you can scan your PC for malware. You can choose different applications and services; for example, Symantec SSL certificates include daily malware scans on your website.
- ✓ **Reassure visitors that your website is secure and scanned regularly.** Trust marks, such as the Norton Secured Seal, can give your website visitors confidence in your website's security.

- **Consider paying for a professional security review of your website.** A comprehensive check by the experts might spot something you might otherwise miss. Think of it like taking your car in for a service. An annual review by a reputable security firm may be enough, but remember to check for vulnerabilities each time you make any major functionality changes to the website.

Website attacks in the real world

If you think these problems couldn't happen to you because your website is too obscure or your company is too small (or too big), think again.

A Russian crime ring used a botnet of hijacked PCs infected with remote-control malware to scan millions of websites for vulnerabilities in 2014.

According to Hold Security, a cybersecurity firm, the criminals were able to break into 420,000 websites using a SQL injection attack and steal 1.2 billion user name and password combinations and a staggering 542 million unique email addresses.

Most of the companies attacked didn't know they were vulnerable and many of the websites remain unprotected.

Chapter 5

Spotting Vulnerabilities in the Foundation of Your Website Security

In This Chapter

- Understanding the risks of poor SSL/TLS implementation
- Differentiating between the kinds of SSL/TLS certificates
- Highlighting the importance of encryption strength

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), the newer version of SSL, are the bedrock of online security. Often referred to under the umbrella term of *SSL,* they're the most important security protocols for the Internet, and their goal is to ensure private communication between your website server and your visitor's web browser.

When a customer enters her credit card details or accesses her order history from your website, that data is encrypted while it's in transit so that no one can read it.

Some SSL/TLS certificates also authenticate the owner of a web domain, reassuring visitors that they're giving their information to the person or business they think they are.

The SSL/TLS infrastructure is strong, but nothing is completely impervious to the guile of a determined, malicious hacker. Some weaknesses exist that criminals can exploit to undermine trust in the Internet. This chapter looks at what these weaknesses are and how to spot and strengthen them in your own website security.

Grasping How Criminals Exploit Poor Implementation

SSL/TLS certificates don't just work. SSL/TLS certificates have to be correctly implemented on your website to work effectively, which isn't always straightforward. When you don't pay attention to detail and keep your implementation software updated, you create vulnerabilities in your security infrastructure, which criminals can exploit.

The following sections look at vulnerabilities in the implementation software that attackers have already exploited. We also look at man-in-the-middle attacks, which are made possible on websites that encrypt some pages but not others and fail to take account of the information transmitted when visitors go between the two.

Exploiting SSL with Heartbleed and FREAK

The OpenSSL cryptography software library is one of the most popular libraries that websites use to implement SSL/TLS certificates. Researchers have found two specific ways that criminals can exploit SSL. They are as follows:

- **Heartbleed Bug:** In 2014, researchers found a security bug in the Open SSL library, named the Heartbleed Bug, which allowed attackers to get information from a website server, using the very software that was meant to keep data safe.
- **FREAK:** Similarly, the FREAK vulnerability, spotted in 2015, was primarily due to a bug in OpenSSL client software and Microsoft's SChannel library. This one, however, was only exploitable on poorly configured web servers.

The only way to fix these vulnerabilities is to update to the latest version of OpenSSL and properly configure your web servers. These are just two examples — there have been others, and there will likely be more in future, just proving that implementing SSL/TLS certificates is far from a one-and-done job.

Exploiting SSL with a man-in-the-middle attack

Most websites only use SSL/TLS encryption on pages where you exchange confidential information, like shopping carts, so that hackers can't eavesdrop on sensitive information.

After a visitor leaves this secure page, however, and moves to one without encryption, there is an opportunity for a hacker to use a man-in-the-middle attack. So, for example, the hacker can use cookies on the unencrypted pages to impersonate a visitor who has previously logged in and access what should be private, secure pages.

TECHNICAL STUFF

A *cookie* is a packet of data sent by an Internet server to a browser, which is returned by the browser each time it subsequently accesses the same server. Cookies are used to identify a user or track his access to the server.

The functionality that cookies provide is good for visitors who want targeted recommendations when shopping or who don't want to have to repeatedly log in to the same website. However, it's bad if those cookies are unencrypted and contain data carried over from secure pages, which allows hackers to impersonate that user.

TIP

Implementing security certificates across your entire website — called *Always-on SSL* — secures a visitor's actions on every page, making it more difficult for criminals to carry out man-in-the-middle attacks.

Eyeing the Dangers of Different SSL/TLS Certificates

SSL/TLS certificates come in a variety of levels, ranging from low to high authentication. There are also reputable *certificate authorities (CAs)* and less reputable ones. Even though cheap or even free certificates will do the job, they often don't come with any extras like insurance, which can be very valuable financially.

These cheap certificates also rarely come with any support, are supported by a weaker infrastructure, and are likely to cost you an extra fee for every little thing you ask for.

The following sections look at the different kind of SSL/TLS certificates that you can get for your website and the key differences around the credibility they offer for your website visitors.

Domain Validated certificates

A *Domain Validated (DV)* SSL is the lowest form of validation. All a DV SSL/TLS certificate proves is the email address and sometimes the name of the person who owns the website.

This low form of validation makes it easy for criminals to set up phishing websites by using a misspelled version of the domain that they're imitating so the website looks legitimate and secure with the familiar SSL padlock and "https" in the address bar that a DV SSL/TLS certificate provides.

Criminals then can trick visitors in to handing over confidential information. For website owners that care about proving their credibility, DV SSL/TLS isn't an option.

Organization Validated certificates

The next level up from DV SSL/TLS is *Organization Validated (OV)* SSL/TLS. OV certificates are harder to obtain than DV because CAs verify that the business requesting the certificate is legitimate before issuing the certificate.

OV SSL/TLS certificates don't just prove that the person who requested the certificate owns the website, they also confirm that person belongs to a verified organization. This certificate offers greater reassurance to your website visitors, something that's particularly important for ecommerce websites.

Extended Validation certificates

Extended Validation (EV) certificates provide the greatest credibility because they require the domain owner to complete detailed and rigorous checks to obtain them.

EV SSL/TLS certificates are only suitable for websites owned by private organizations, government entities, and business entities — in other words, any organization that has to register itself with a trusted third party, such as a local or national government organization.

When you implement EV certificates, the address bar of your visitor's browser will turn green, differentiating your website from those who use DV SSL/TLS or OV SSL/TLS certificates.

Although they're the most credible, not all websites need the level of authentication that EV SSL/TLS provides. The more popular your website and the more sensitive the information you are asking for, the more likely it is that EV SSL/TLS will benefit your business.

Exploiting Weak Encryption: What Criminals Do

Even though different types of certificate offer different levels of authentication, within each of those types of certificate there are also different strengths of encryption. Different CAs offer a different standard, and it's worth checking exactly what they're offering you.

REMEMBER

The strength of an SSL encryption depends on the algorithm used and the length of the key, measured in bits. So basically, hackers can more easily crack the encryption on websites that have certificates with a shorter key, using a brute force attack.

The higher the number, the more computer power and time a criminal needs to hack the encryption. As computing power has improved, so certificates have become stronger to resist being cracked. Reputable CAs therefore no longer issue 512-bit keys, and the industry standard is now a minimum of a 2048-bit key.

Strength in numbers

Computing power has increased considerably in the last few years. Although people can access more services and complete more transactions online and scientific advances can progress at a faster pace, this increased computing power also gives cybercriminals an advantage.

The more computing power criminals have at their disposal, the faster they can hack a password or break hashing algorithms used to encrypt data. They simply set a program running that tests all the possibilities until it hits at the right one, which is called a *brute force attack.*

The cyber security industry is therefore always working to make its security offerings stronger in order to stay one step ahead of the criminals computing power.

The strength of SSL/TLS in particular has come a long way since 1994, when the first online transaction took place. In the last few decades, it has become easier for criminals to crack hash functions, thanks to the increased availability of incredible computing power.

Because experts were worried that criminals could now crack SHA-1 algorithms, 2015 saw the switch from SHA-1 to SHA-256, moving the industry standard along considerably.

The old standard for SSL/TLS, SHA-1, produces a 160-bit hash value known as a *message digest.* On the other hand, SHA-256 produces a 256-bit hash value. In other words, SHA-2 is much harder to crack.

Chapter 6

Reducing Unnecessary Vulnerabilities on Your Website

In This Chapter

- ▶ Making sure you manage SSL/TLS properly
- ▶ Keeping your website technology up-to-date
- ▶ Securing your site with good management

You're safe to assume that at one point or another, your website will fall victim to an attack. How bad the consequences of that attack are depends on how well prepared you are.

Failure to take proper care of your technology certainly causes vulnerabilities. To avoid not being prepared, you need to understand how your website technology works, where its weaknesses are, and how to prevent them.

Not knowing how to handle an attack is a vulnerability in itself, so this chapter looks at how you defend your site, and your business, with good, basic website security and maintenance.

Managing SSL/TLS Certificates

Not all certificate authorities (CAs) are created equal. Proper SSL/TLS certificate management starts with choosing the right partner. If you go for the cheapest you can find, then you'll get what you pay for in terms of reliability.

Beyond that, you need to be aware of several elements to implementing and maintaining your certificates. These sections point out two main actions you can take to make sure your certificates do their job and keep customer information encrypted in transit and your visitors reassured.

Renewing SSL/TLS certificates

One of the easiest ways you can protect your visitors' information is to make sure you renew your SSL/TLS certificates on time.

When people access a site with an expired SSL/TLS certificate, they see a warning, telling them the site may no longer be secure. The advice for consumers: if this warning pops up, don't proceed to the site in question because any data shared may be vulnerable to interception.

You don't want your potential customers to see this warning when visiting your site.

TIP

The good news is that renewing your SSL/TLS certificates is easy. All you need is a little advance planning. Having the certificate renewed can take a couple of weeks, depending on the level of certificate you apply for (refer to Chapter 5 for the different levels), so don't leave applying to renew your certificate to the last minute.

WARNING!

Extended Validation (EV) certificates, as we explain in Chapter 5, involve a great deal of authentication — a process that inevitably takes time. If a company claims to be able to fast track this process, take a moment to question on how — you may just find you're not getting what you pay for.

REMEMBER

Management software is available that sends automatic reminders when your SSL/TLS certificate is about to expire, so you have no excuse not to stay on top of it.

Patching and updates

Patches and updates are the bread and butter of website security. When hackers find a weakness they can exploit, vendors quickly issue a patch to limit the damage.

Your site is only made safe, if you install and run these patches and updates. Otherwise, criminals can carry on exploiting the weakness.

This advice applies to server software, content management systems, and SSL/TLS libraries — anything that you use to help your site run.

In 2015, 54 zero-day vulnerabilities were found, according to Symantec's Website Security Threat Report (WSTR), a 125 percent increase from the previous year. These are vulnerabilities in commonly used software that criminals discovered before the software creators did. (Refer to Chapter 3 to find out what criminals can do with zero-day vulnerabilities.) What's more concerning, however, is that the majority of malicious attacks in 2015 took advantage of vulnerabilities for which a patch already existed, but site owners had failed to install.

Keeping Servers Safe: Antivirus and Antispyware Software

You need up-to-date antivirus software on all individual devices, including servers. Doing so helps to mitigate unpatched vulnerabilities (not that you should have any other than zero-day vulnerabilities) and warns you when malware is trying to attack your devices.

Often, however, malware is designed to go undetected. So for the times when it slips under the radar, you need antispyware software to help you keep an eye on data being sent in and out of your servers.

With antispyware software, you can monitor traffic and spot unusual requests or sensitive data going out that shouldn't be and respond to breaches or signs of malware infection much quicker.

Make sure you only buy antispyware and antivirus products from a retail store or a trusted online provider. Some programs available to download are actually malicious spyware in disguise.

Maintaining Good Management Practices

Good security isn't just about technology; it's about people and process too. You need defined processes, and you and your employees need to stick to them. The following sections identify some sound practices your business can take to ensure your website's security.

Managing passwords

Good password security is such an obvious security measure, yet people still don't update their passwords regularly. In fact, many people use the same password for multiple accounts according to the WSTR 2015; in effect creating a master key if a criminal gets hold of it. Good password management is critical, and you can find best practices for this in Chapter 4.

Poorly managed email account passwords is one thing, but not having strict security measures for your SSL/TLS private keys — the string of data used to decrypt confidential information — is an even more serious issue. If a hacker gets the passwords that provide access to those keys, then all your encrypted data is accessible. So limit access and consider two-factor authentication to increase their protection.

Defining access

To limit the likelihood of losing passwords or keys, keep the following suggestions in mind:

- ✓ **Be strict about whom, if anyone, has access to them.** By developing tiers of authority and only giving access on a need-to-know basis, you can control risk.
- ✓ **Implement two-step authentication for access highly secure data, like SSL/TLS keys.** This means not only having a password, but also an additional passcode that is generated at the time the user wants to log in and is usually sent either to his email address or mobile phone.

- **Consider two-factor authentication.** This goes beyond two-step authentication, as we talk about in Chapter 5, and requires two factors out of something you know, something you have, and something that is inseparable from you, like a fingerprint.

  So a text sent to your phone isn't a different factor from a password because it's still something you know — the phone itself didn't generate the passcode — so the phone itself isn't a factor. A passcode generator, however, like you get from some banks, is a different factor and together with a password would form two-factor authentication.

Executing employee onboarding and exit procedures

People will come and go from your business. Onboarding new employees and training them on good security practices is important, but tying up all loose ends with employees that leave is also crucial for you to do.

TIP

When someone joins your organization, do a background check, even if only calling on their references to make sure that they're genuine. If your site gathers sensitive or personal details and your new employees will have access to that data, run a criminal record or background check on them as well.

TIP

For when employees leave, have an established list of all systems that employees use and who has access to what so you can revoke access and change passwords. Whether they leave on good terms or not, you don't want your valuable data accessible to the wrong people.

The Panama Papers leak: A vulnerable website server example

Web servers make up part of the infrastructure behind a website. Using common protocols, which are predefined methods of communication, web servers transmit data to your visitors' computers. The most common method in HTTP (Hypertext Transfer Protocol) is GET, which tells the server to retrieve a specific file. It's this communication between server and client that SSL/TLS certificates encrypt.

While SSL/TLS infrastructure is a common target for hackers, the number of malware attacks designed to target web servers has greatly increased. Hackers have realized that these web servers are just as valuable as the information encrypted by SSL/TLS certificates.

One of the most publicized web server attacks of 2016 was the Panama Papers leak, which saw Panama City–based law firm Mossack Fonseca suffer a significant data breach, exposing the tax dealings of clients including world leaders and celebrities. According to a report in *Wired* magazine, experts believe the breach was caused by a series of unpatched vulnerabilities, including an out-of-date WordPress plug-in and obsolete SSL protocols.

This demonstrates what the fallout of a web server attack can look like and how crucial it is to perform regular maintenance on your servers and update vulnerability patches as soon as vendors issue them.

Chapter 7

Getting Savvy to Scams

In This Chapter

- Understanding why criminals use scams
- Outlining the tactics criminals use to scam your employees
- Knowing how not to fall into their trap

For criminals, luring a company's employee into giving away sensitive information is much easier than mounting a full-scale attack against a website.

Without the proper training, one of the biggest risks to your website's security is your employees. Even the most dedicated, trustworthy, intelligent staff members can become accidental participants in a cyber attack if they don't know what to watch out for.

Of course, rogue employees are also a risk, which we talk about in Chapters 3 and 6, but this chapter focuses on employees who mean no harm, but whose ignorance could cost your business dearly as they fall prey to criminal scams without even realizing it.

Innocent mistakes can quickly lead to devastating attacks. For instance, the 2013 Target data breach was caused in part because at least one employee of Fazio, one of Target's third-party vendors, was tricked into installing malware by a phishing email scam, according to ZDNet.

Criminals use highly sophisticated scams to trick people. This chapter looks at some of the most common ways employees can fall victim to a criminal's trap and put your website at risk and what you can do to ensure your employees don't fall victim.

Knowing What Phishing Is

Phishing involves sending mass emails or other communications, like social media messages, to certain targets in the hope that some of the recipients will take the bait.

To fool their victims, criminals ensure the messages look like they're coming from a legitimate business or reputable individual. The days of questionable spelling and princes from Africa are gone; modern criminals write articulate emails using logos and pictures, just like any other business.

The aim of phishing is usually to get the victim to download the attached malware, which may look like an invoice, or to follow a link to a malicious website.

The ultimate goal is to get malicious software onto the victim's machine or to get him to enter secure login details onto a phishing website, while thinking he is logging into the real website.

WARNING!

Many people think they can identify whether a linked website is safe or not by simply reading the URL and seeing if it matches what they think it should be. Attackers are clever though; they have two tricks up their sleeve to counter this:

- **Criminals can compromise subdomains of a trusted website.** Meaning the URL looks official, but the content on the page won't be. For instance, `www.example.com` may be completely safe, but attackers may have secretly compromised `www.scam.example.com` and installed malicious code.
- **Criminals deploy a homograph spoofed URL.** A *homograph-spoofed URL* is a web address that uses alternative characters to make it read like a recognizable URL, when it's actually a completely different one. Look at Figure 7-1. Can you tell the difference between these two web addresses at first glance?

The best weapon against scams is training and a robust IT security policy that you actively enforce. Chapter 9 looks at employee training in more detail.

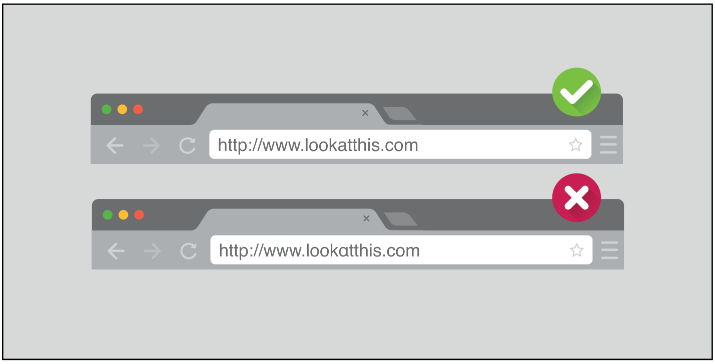


Figure 7-1: Criminals use homograph-spoofed URLs like this.

By using slightly inaccurate spelling or, as in this example, a different font within a URL, a cybercriminal could register a domain and replicate a legitimate website for malicious purposes.

Considering How Spear-Phishing Is Different from Phishing

Phishing scams cast a wide net in the hope a certain percentage of victims will be fooled. *Spear-phishing,* on the other hand, is a highly targeted scam, where the criminal sends an email to one individual or a few members of the same organization.

With a smaller number of targets, criminals executing these scams are much craftier, often:

- Researching their target using search engines and social media to see if there are any details they can use to establish themselves as someone who knows the target.
- Posing as a colleague, a friend, or a business the victim has recently worked with.
- Requesting an urgent or important action that will cause the victim to let their defenses down and feel compelled to help.
- Targeting someone senior from an organization in a scam known as *whaling.* A "big fish" (or more accurately, a big marine mammal) in the company can provide access to more valuable information.

REMEMBER

Perhaps Susan from accounting really did forget her intranet login details and urgently needs them. Maybe you're late paying that invoice from your accountant's firm. Nonetheless, you should always contact the sender through an alternative channel to verify the email is actually coming from who it says it is.

TIP

You can easily forget just how much information a simple search engine search can reveal about your business and you. Make it harder for hackers and limit the amount of unnecessary private information you publish online.

Examining Social Engineering in Greater Depth

Social engineering comes in a variety of different forms, but the aim is essentially always the same: to trick people into bypassing their normal security procedures and their own common sense.

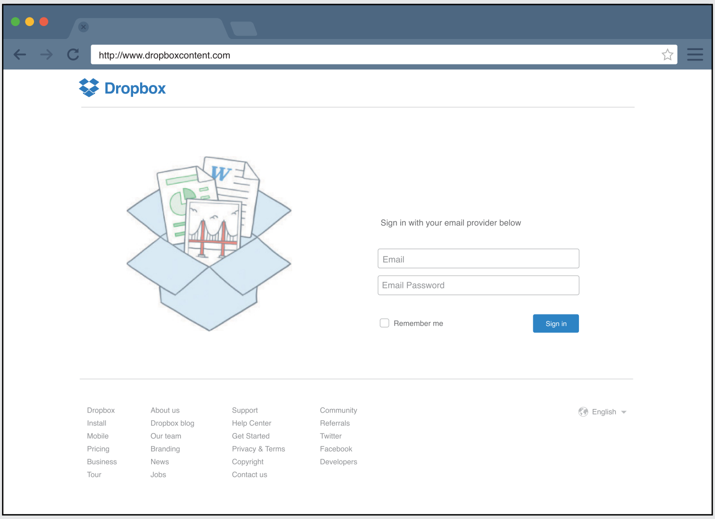
Phishing and its variants are examples of social engineering scams, but the scammer's toolkit doesn't end there. They also use the following:

- **Baiting:** Commonly an attacker leaves a USB stick near a target's workspace. When the target picks up the USB device and plugs it into his computer to see what's on it, malware automatically runs and installs on his computer, possibly infecting the entire network.
- **Quid pro quo:** Often this attack involves the scammer impersonating a business's IT support service and ringing all the numbers in that business until the scammer reaches someone who has asked for IT support. Because the victim was expecting the call, she happily follows the disguised attacker's instructions to fix her IT problem. Of course, what those instructions are actually doing is leading the victim to open up access to her IT systems or download malware onto her PC.
- **Scareware:** Unsurprisingly, fear is the name of the game with scareware. An attacker may pose as a security authority — like an antivirus provider— and warn the target that he has accidentally downloaded malware. Handily, the attacker will have just the solution to the problem: his own malware download disguised as a program to delete the made-up one.

Phishing scams come in all kinds of disguises

The whole point of a phishing scam is to fool you into thinking that you're logging into a legitimate website that you know well and use often. And for that reason, criminals go to a lot of effort to make these fake websites look convincing.

A scam targeting Dropbox users managed to create a fake login page hosted on Dropbox's user content domain (like where shared photos and other files are). This page was even served over SSL, making the attack more dangerous and convincing. Take a look — can you spot it was fake?



http://www.dropboxcontent.com

Sign in with your email provider below

Victims were sent an email with the subject "Important," claiming that they had been sent a document that was too big to send over email and that they needed to click the link to retrieve said document. After a victim had entered her details into this fake Dropbox page, she was simply redirected to the real login page. There was, of course, no document to retrieve.

Similar scams have been set up to try and steal login credentials for WordPress websites. In one example, victims were sent an email from wordpressplugin@hotmail.com with the subject: [WordPress.org Plugins] Urgent: Your Plugin Has Been Removed DO NOT RESPOND.

The email then warned the recipient that a plugin had been removed from her website and to follow a link to find out more information. The link, again, took the victim to a phishing website in the hope that she would enter her login credentials, and in effect hand them straight over to the criminals.

Chapter 8

Tackling the Takedown: DDoS

In This Chapter

- Comprehending how a DDoS attack is carried out
- Understanding the motivations behind DDoS attacks
- Making sure you're prepared for an attack

Distributed Denial of Service, or DDoS, is a way for hackers to attack websites by overloading them with more traffic or data than the servers can handle.

A DDoS attack uses the power of botnets, like we discuss in Chapter 4, to flood a victim's website with access requests, effectively taking the website offline.

DDoS attacks are different from most other website threats because they don't directly breach the security of your website. They are nonetheless a threat, and this chapter explores how they work, why they're used, and how you can prepare your website for an attack.

Grasping How DDoS Attacks Work

You don't have to own a botnet army to carry out a DDoS attack. Thanks to the black market, anyone can hire a botnet for a certain period of time or for a particular attack and carry out an attack for as little as $10 to $1,000 per day.

Depending on how powerful an attack is, the flood of traffic created by the botnets can also cause collateral damage to other websites hosted on the same server or by the same hosting engine.

Think of it like a party. The aim of the DDoS attack is to make the buffet table inaccessible so the attacker floods the party with guests all trying to reach the buffet table. By flooding the party though, the attacker not only blocks access to the buffet by making the room so full no one else can get to it, but also blocks access to the bar and the dance floor because the party is so full that no one else can get in through the front door.

Figuring Out Why People Use DDoS Attacks

Knowing the different reasons why someone might attack is important, because you can know better how to respond if you're ever made a victim.

Because there isn't much else a DDoS attack can do other than shut down a website, people do it mostly to disrupt, protest, or hold an organization or individual to ransom. The following sections examine in greater depth the reasons why hackers use DDoS attacks.

Cyber heists

Holding a website ransom until the owners pay up is the most lucrative reason someone would launch a DDoS attack. Some attacker groups even hold businesses to ransom with just the threat of an attack.

Commonly malicious hackers request ransom payment in the crypto-currency Bitcoin, currently valued at $587.30 per coin. Criminals have been known to request a ransom of anything up to 40 Bitcoins ($23,434.40) from big companies. Using a digital currency makes the payments harder to trace and the criminals harder to catch.

WARNING! Even if you pay up, you can't be certain that you won't be attacked anyway. Surrendering to a DDoS ransom generally isn't a good idea because threats can escalate and increase in price if you're seen to be compliant.

Just for kicks

Another common motivation is simply the desire to cause mayhem. On New Year's Eve in 2015, the BBC website was targeted by a DDoS attack. The main website and iPlayer services went down for a few hours, disrupting key services for thousands of visitors worldwide. A group called New World Hacking claimed responsibility, saying they carried out the attack as a "test of its capabilities."

The BBC were able to handle the knock to their reputation and the cost of getting back online, but if a smaller company suffers a malicious attack it could damage their reputation at best and put them out of business at worst.

Proving a point

Some attackers want to cause mayhem not for fun, but to make a point. They tend to choose their target because of a specific political or social reason. The attacker in this case wants to cause difficulty for the victim and raise publicity for the issue they care about.

When WikiLeaks' founder Julian Assange became the center of a criminal investigation in 2012, for example, his supporters reacted by launching a DDoS attack on MI5's website, which went down for several hours.

The one-two punch

The most sinister reason criminals use DDoS attacks is as a distraction while they carry out a more serious attack that does breach your website security.

Although system administrators are grappling to get a website back online during a DDoS attack, the real attack is happening elsewhere, infecting systems with malware or stealing data or money.

On Christmas Eve in 2012, for example, Bank of the West in California was victim to a large DDoS attack that distracted staff while criminals carried out a $900,000 heist on one of its client's accounts.

Preparing for a DDoS Attack: The How-To

Thanks to the growing reliance on technology and the proliferation of Internet-connected devices, DDoS attacks have never been easier to carry out or more damaging.

Now that devices like fridges and TVs can be hacked, people can build ever-bigger botnet armies, with one recent attack using 900 CCTV cameras to power their attack.

No website is immune from a DDoS attack. Any public service or website is vulnerable to upsetting the wrong person or just being in the wrong place at the wrong time.

TIP

To improve your website's security, be prepared and do the following:

- **Make sure you have network-monitoring tools that notify you of unusual amounts of traffic or unusual sources.** There are several different kinds of DDoS attack — each exploiting a different kind of network request or flooding particular ports. Understanding these different types of attacks requires technical expertise, but specialist firms have tools that can spot specific types of traffic and requests coming to your website server that would indicate the start of an attack. If you run your own web server, it's also worth getting to know your typical inbound traffic profile so you can spot when something out of the ordinary is happening.
- **Know how to isolate certain services to help restore essential access for customers.** Do you have access to a backup server that you can run essential services from while your main server remains under attack? Can you block certain types of traffic without cutting off access for your customers? If you host your own web server,

you need to understand your IT setup well enough to answer these questions.

- **Create a list of important systems and services that make up your website and assess the potential impact of an attack.** For example, not only was the BBC website hit in 2015, but its iPlayer service was taken down too. If your product is an app hosted on your website, then you need to know how to restore access to it, perhaps before your main website, because it'll have a bigger impact on customers. Maybe retrieving account information is more critical than getting your app working. The point is you need to know so that you know how to respond and what to focus on first.
- **Create a DDoS Playbook that includes this information:**
  - Names and numbers for your mitigation service — who can handle larger DDoS attacks — and your Internet service provider (ISP)
  - A list of questions to ask your ISP or web host, including what protocols they have in place for a DDoS attack, how they mitigate an attack, and what their maximum bandwidth is
- **Consider cyber insurance.** This insurance can mitigate the risk to your business of an attack. (Refer to Chapter 1 for more information.)

Being prepared reduces panic and helps you make measured, practical decisions on which systems to safeguard or restore first when you're attacked.

You also need to keep website visitors and customers informed through other channels, like your Twitter feed or Facebook page; or if you're a software developer, for example, you could use your GitHub account to create a Gist page, like Basecamp did, about what is happening, what you're doing to fix things, and how long you think it will take.

Protecting against DDoS attacks

Symantec has partnered with Incapsula to make its Complete Website Security solution more effective than ever by including protection against DDoS attacks.

Working from a cloud-based system, the DDoS protection service doesn't need any extra hardware or software installed and works constantly in the background to monitor any suspicious traffic that may point to a future attack.

The Imperva Incapsula service also offers enterprise-grade web application security, performance optimization, and load balancing. The Web Application Firewall (WAF) protects websites from multiple kinds of attack, including cross-site scripting (XSS) and SQL injection.

Chapter 9

Ten Top Tips for Keeping Your Website Secure

In This Chapter

- Finding the right advice
- Taking the right security precautions
- Educating your employees

The threats to your website are real and varied, but there are plenty of ways to protect against them. Some are technology-based, some are process-driven, and others are about behavior and mind-set.

You can't be too careful. That's why, in this chapter, we gather ten top practical tips for keeping your website secure.

Read The Website Security Threat Report (WSTR)

Protecting your website is much easier if you know what you're protecting it from. Although this book covers the essentials, the world of online security is always evolving. Criminals come up with new tactics, and security organizations like Symantec come up with new ways to defend against them. The best way to stay on top of it all is to read the Website Security Threat Report (WSTR).

Every year Symantec produces this in-depth report on the current threats facing websites just like yours. It talks about trends over the previous year, gives specific examples of what to look out for, and explains why these threats matter to your business and the economy as a whole.

Check out Symantec Connect

Another way to stay up-to-date with breaking news in the world of website security is through Symantec Connect (`www.symantec.com/connect/`).

Your website may have been exposed to a new zero-day vulnerability or a new kind of scam targeting website administrators. Symantec Connect is a community of customers, partners, and employees all offering insights and expert advice on Internet security and keeping you in the know.

Have a Plan

Preparation is half the battle. Know your website systems inside out and decide who is responsible for what in the event of an attack, and you can actively reduce the impact of a possible attack.

You need to think about the following:

- ✓ Who you need to contact for help mitigating an attack
- ✓ What bodies you need to inform
- ✓ How you are going to get in touch with customers
- ✓ Who has which passwords
- ✓ Who all your IT partners and providers are, including your ISP and web-hosting engine (if you use one)

Consider Your Whole Ecosystem

Your website isn’t just a server and a content management system. It’s a whole ecosystem, which is often tied to your wider IT through networks and databases.

For example, have you deployed a web application firewall to defend against injection attacks? Is your code signing secure for your web apps? If you develop apps, do you sign them digitally? Are your signing keys secure? Do you have automated tools to detect and defend against the increasing threat of DDoS attacks? Make sure you understand the bigger picture and can see where one weakness might lead to another.

Scan Regularly

Keep an eye on your web servers and watch for vulnerabilities or malware. Plenty of automation tools are available to help you with this scanning.

Many companies, including Symantec, offer free vulnerability and malware scanning with some of its SSL/TLS certificates.

Be Picky about Your Plug-Ins

The software you use to manage your website comes with vulnerabilities, as we talk about in Chapter 4.

The more third-party software, apps, and plug-ins you use, the greater your attack surface; as a result, only deploy what's absolutely necessary, and make sure you do your research about which have the best security policies and provide the most frequent updates.

Update Servers, CMS, and Other Website Software

No matter how much research you do, even the best software will have vulnerabilities — it's just the nature of coding complex programs.

That's why companies and creators regularly release patches and updates. But they'll only fix your weaknesses if you actually install and implement them, so keep on top of it. Have a regular update schedule, and don't let any slip through the cracks.

Protect Cryptographic Keys

If someone gets hold of your SSL/TLS certificate keys, then it's game over (cryptographically speaking). Attackers with this information can unencrypt all the personal information you've exchanged with your customers via your website. You therefore need to keep those keys — known as *private keys* — under lock and key (as it were) and control access to them very carefully. Only let those who absolutely need access to them have it and implement two-factor authentication for added security.

Educate Employees

As ever, basic common sense and the introduction of some good security habits can go a long way to keeping your website safe. When it comes to training, start with the basics:

- **Ensure employees don't open attachments from senders they don't know.** Many scams and malicious emails come with an attachment that looks innocent but is actually code that will run as soon as someone opens the attachment.
- **Educate them on safe social media conduct.** Offers that look too good to be true probably are. Hot topics like celebrity gossip are a favorite source of bait for scammers, and not all links lead to real login pages.
- **Encourage them to adopt two-step authentication on any website or app that offers it.** When they sign in using a password, they'll be sent a passcode, usually to their phone, which they need to enter before the website allows them in. This way, even if a criminal has their password, they still can't access sensitive information.
- **Ensure they have different passwords for every email account, applications, and login, especially for work-related websites and services.** Get them to change them regularly.
- **Remind them to be cautious online**. Having antivirus software doesn't mean it's okay to go on malicious or questionable websites. And often phishing websites look very similar to legitimate ones so they need to stay vigilant at all times on the web.

- **Apply effective access controls to protect servers and private keys working on a least-privilege basis.** Unless someone needs access to a server or system to carry out his job, then he shouldn't have access to it. The fewer people who have access to a password, the lower the risk is that it will get lost or leaked.

  Beyond that, *least-privilege basis* means that even within an application or system, people only have the privileges they need to do their job without hindrance. For example, you may only give someone access to view a document, but not to edit it. Or you may prevent non-admin users from downloading software onto a machine if all they need to be able to do is run backups.

Read Website Security For Dummies

Understanding in greater depth how the different security measures you can implement actually work is important — in particular, the foundation of website security, SSL/TLS certificates.

Website Security For Dummies, Symantec Special Edition, covers exactly this topic. It can help you pitch website security to your boss in business terms and help you tell your OV from your EV and your private keys from your public ones.

Glossary

Always-on SSL: This refers to the practice of implementing SSL/TLS certificates on every page of your website so that every interaction a visitor has with your website is encrypted. Many major brands and institutions have implemented always-on SSL, including Facebook and the White House.

Antispyware: A type of software designed to detect and remove unwanted spyware programs. *Spyware* is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them.

Bitcoin: This is a type of digital currency (or crypto-currency) that has real value like any other currency. No state, government, or bank backs it; instead it's a peer-to-peer payment network, powered by its users and with no central authority or middleman.

According to the Bitcoin website, "From a user perspective, Bitcoin is nothing more than a mobile app or computer program that provides a personal Bitcoin wallet and allows a user to send and receive bitcoins with them. . .behind the scenes, the Bitcoin network is sharing a public ledger called the 'block chain.' This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction."

Bits: In computing, a bit is a unit of information expressed as either a 0 or 1 in binary notation.

Bot: Bots are simple computer programs that can run autonomously and automatically over the Internet and that carry out simple, repetitive tasks.

Botnet: A botnet is a group of Internet-connected devices, traditionally computers that attackers have infected with malware. This malware then allows them to control the devices remotely. These networks can be vast, involving hundreds of thousands of devices.

Botnets-for-hire: Criminals can hire botnets that other criminals have already established in order to carry out, for example, specific spamming campaigns or distributed denial of service (DDoS) attacks. These services are available on the black market, often arranged via the dark web.

Certificate authority: This is an organization that issues digital certificates — or SSL/TLS certificates — to website owners.

Cookie: A yummy treat favored by blue monsters. In the context of websites, though, a cookie is a packet of data that an Internet server sends to a browser, which the browser returns each time it subsequently accesses the same server. Cookies are used to identify a user or track her access to the server.

Cross-site scripting (XSS): When a criminal gains access to your website and adds malicious code to the code already running, it's known as cross-site scripting. This code can do all kinds of things from accessing a visitor's webcam to redirecting visitors to a phishing website.

Cryptographic keys: A cryptographic key is a string of *bits* used by a cryptographic algorithm to encrypt plain text. They're integral to how SSL/TLS technologies work. You, as a website owner, create a pair of private and public cryptographic keys. You keep the private keys as a closely guarded secret because they are what allow you to unencrypt the information you receive from website visitors. However, you send the public keys to a certificate authority when you apply for a SSL/TLS certificate in order for it to validate those keys as being associated with your certificate.

Cyberespionage: Cyberespionage aims to gather confidential information, state secrets, or similar sensitive data without the owner knowing. The difference from regular espionage is that cyberspies carry it out over computer networks rather than physical spies sitting on park benches pretending to read the paper.

Dark web: The dark web refers specifically to a collection of websites that hide the IP addresses of the servers that run them. You need particular software or authorization to access them, and working out who is behind the websites is extremely difficult.

Many websites on the dark web hide their identity using the Tor encryption tool. You can use Tor to hide your identity and spoof your location. When a website is run through Tor, it has much the same effect. Although innocent people concerned about their privacy and data security use the dark web, cybercriminals and espionage organizations also tend to operate via the dark web, because it offers the cover of anonymity.

Distributed denial of service (DDoS) attacks: This attack is a way for criminals to take down a website by overloading it with more traffic or data than the servers can handle. It doesn't breach security, but it does cause significant disruption and damage.

Hacktivist: Hacktivist is a British rap metal band from Milton Keynes, Buckinghamshire, England, formed in 2011. Of course, in the world of cyber security, a hacktivist is someone who gains unauthorized access to computer files or networks in order to further social or political ends.

Malvertising: Malicious or malware-infected advertising is a method criminals use to get malware onto otherwise secure and reputable websites. Criminals submit ads that contain hidden malware to (often unwitting) ad agencies, which then upload and distribute the ads to display on innocent websites.

Malware: Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.

Man-in-the-middle attack: An attack in which an attacker is able to read, insert, and modify messages between two users or systems. The attacker must be able to observe and intercept messages between the two victims.

OpenSSL: According to its website, "OpenSSL is an open source project that provides a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It's also a general-purpose cryptography library."

Patch: A patch is a software term for a type of programming code. When software developers notice a problem with their software or a security flaw in the coding, they write new code to patch the flaw. Then, after they've tested it, they release the patch for you to download and install.

Payment Card Industry Data Security Standard (PCI DSS): This is a worldwide standard that the major credit card brands including VISA, MasterCard, American Express, Discover, and JCB set up to help businesses process card payments securely and reduce card fraud.

Personally identifiable information (PII): This is a legal term that refers to any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Phishing: This involves sending mass emails or other communications, like social media messages, to certain targets in the hope that some of the recipients will take the bait and end up revealing sensitive information or passwords.

Phishing website: This is a website designed to look like a well-known or established website — in particular the login page. Its purpose is to fool a visitor into entering their login details, which criminals can then either use or sell.

Ransomware: Ransomware is a type of malware that encrypts files on your computer so you can't open them anymore or locks your whole device and then demands a ransom fee, which may or may not actually unlock the files or device.

Script kiddies: This is a rather derogatory term: it means a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.

Spear-phishing: This is a highly targeted scam, where the criminal sends an email to one individual or a few members of the same organization in attempt to scam them or get them to download malicious software. They're often well researched and highly polished.

SQL: SQL stands for *Structured Query Language,* and it's a specialized language for updating, deleting, and requesting information from databases. In a distributed database system, a program often referred to as the database's *back end* runs constantly on a server, interpreting data files on the server in the form of tables, columns, rows, and fields. Programs on client computers allow users to manipulate that data using SQL. Client programs send SQL statements to the server and the server then processes these statements and returns result sets to the client program.

SQL injection: An SQL injection is a type of website attack. An attacker can exploit vulnerabilities in how your forms are coded on your website and insert a request in SQL that your database responds to. They can ask it to send user names and passwords or other sensitive data that you don't want getting into the wrong hands.

SSL/TLS: Secure Sockets Layer and Transport Layer Security are the standard security technologies for establishing an encrypted link between a web server and a browser.

SSL/TLS certificates: You need to properly install SSL/TLS certificates in order to establish encrypted communication between your website and your visitor's browser. Certificates also authenticate your website server. Different levels of website owner validation are vailable with SSL/TLS certificates, depending on the type you purchase.

Trust marks: Trust marks, such as the Norton Secured Seal, reassure your website visitors that your website is secure and scanned regularly. They're often available from the same security partner that provides your SSL/TLS certificates.

Two-factor authentication: This is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both factors. It's like needing both an ATM card and a personal identification number [PIN] to retrieve money from a bank account.

Vulnerability scanners: This is software that can scan the various pieces of software that make up your website and spot vulnerabilities and exposures that criminals could exploit.

Watering-hole attack: Sometimes criminals want to target very specific individuals or people from a particular organization. In order to do this, they find a website that they know the person (or organization) in question visits regularly and hacks it to install malicious code that will infect those visitors. Some code is so sophisticated that it can recognize the IP address of a visitor and only trigger the malware to download if the visitor is from the target organization. This reduces the risk that someone will detect the malware and remove it.

Web attack toolkits: Available on the black market, these contain everything a criminal needs to carry out an attack on your website. They include software that scans for vulnerabilities, droppers to download the relevant malware onto a website, and the malware itself. There is no need for the attackers to have advanced code-writing skills — it's all done for them and available in the same way reputable software-as-a-service is available to businesses today.

Zero-day exploit: Zero-day exploits are attacks that target the software vulnerabilities attackers discover before the software provider has spotted them and managed to release a patch to fix them.

Zero-day vulnerability: These are weaknesses in a piece of software that the writers of that software haven't realized are there. At the point, a criminal exposes this kind of vulnerability in order to exploit it, the software developer has had zero days to try and fix it — hence the name.

Knowledge is power: website threats are business threats

Your website is critical to your business — whether it's for ecommerce, marketing, or use of your app. An attack could destroy your business, and nobody's immune, big or small. This guide helps you keep your website safe by explaining the threats it faces, how they work, and the best ways to defend against them.

- ***Calculate the cost** — Get to grips with the different ways that a successful attack costs your business time and money, from immediate fixes through to fines and reputation damage*
- ***Get to know the attackers** — Understand who is targeting your website, why they're doing it, and how*
- ***Understand your vulnerabilities** — Discover how attackers find and exploit weaknesses in your website and how you can patch, protect, and prevent with the right technology, process, and people management*

Symantec: Symantec Website Security (www.symantec.com/website-security) provides industry-leading security for websites, data, and applications with SSL/TLS, certificate management, vulnerability assessment, WAF/DDoS, malware scanning, and such. The Norton Secured Seal and Symantec Seal-in-Search assure customers they are safe to search, browse, interact, and buy. Symantec Website Security's sophisticated solutions offer the promise of a safe and trusted Internet experience across all websites and applications.

Open the book and find:

- The cost to your business of an unprotected website
- Who attackers are and what they want
- Tools attackers use and the weaknesses they exploit
- How to protect your website and eliminate vulnerabilities

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-27539-8
Not for resale