10 Don'ts on Your Digital Devices

The Non-Techie's Survival Guide to Cyber Security and Privacy

Daniel G. Bachrach
and Eric J. Rzeszut

Apress

For your convenience Apress has placed some of the front matter material after the index. Please use the Bookmarks and Contents at a Glance links to access them.

Apress®

Contents

Introduction

We hear it every day, on television, on the radio, at the grocery store, and at the movies—that our world is getting smaller. We can be anywhere in the world within a day, by jumping on a plane, and with Skype, Google Hangouts, or Apple's FaceTime we can talk face to face to almost anyone in the world with broadband in the time it takes to turn on the computer or other mobile device. We can get any book, magazine, journal article, movie, television show, or newspaper going back more than a hundred years, and we have essentially limitless, immediate access to all of the publicly available recorded information from the beginning of modern record keeping.

Almost any and all information that we could possibly ever need or want is available to us at the speed of electricity, and our lives are infinitely better for it in uncountable ways. Research and practice in medicine, science, health, art, music, language, travel, and a myriad other domains has increased exponentially as a direct consequence of the immediate availability of information that we take for granted in the 21st century.

While we all take advantage of this magnificently available connectivity in different ways, the overwhelming sociological trend across race, age, gender, generational, and other demographic categories is that as a society we're becoming more connected to one another and not less. In fact, virtual connectivity has become so ubiquitous a concept in our culture today that variation in our levels of virtual connection to one another has come to be recognized as an element of human personality.

For example, recent survey research reported by Broadcom Corporation on more than 2,500 American adults identified seven distinct "connectivity personality types." Nearly half of those participating in the Broadcom survey were identified as either "Always On," "Live Wires," or "Social Skimmers," all of whom maintain very high levels of Internet presence. In contrast, only 2 percent of those surveyed fell into the "Never Minders" category, with essentially no level of social media or Internet interaction whatsoever. The overwhelming majority of us are, apparently, connected at least sometimes to the overwhelming majority of us online.[1] As a society, we're being collectively redefined at least in part by our patterns of virtual interconnection.

[1] BusinessNewsDaily, Chad Brooks, "What's Your Technology Personality Type?" www.businessnewsdaily.com/3557-technology-personality-types.html, December 10, 2012.

Living in the interconnected world we've created and defined carries risks with it, and sometimes potentially very steep costs and difficult-to-recover-from consequences as well. We essentially now live in a globally connected virtual neighborhood and the immediacy and connectedness we enjoy on the one hand directly implies that the neighborhood isn't always safe—not in the conventional sense. Not everyone living in the globally connected community that defines most of our lives in a broad range of fundamental ways is thinking about it in an adaptive, collective-goods focused way.

> *There are thieves who with criminal self-interest and purposeful guile would do you harm and steal your last dollar and good name if given the opportunity to do so. Unfortunately, on the other side of the wireless network connecting you to libraries and shopping and books and movies and friends and all of the data you use every day are criminals who are actively trying to steal your passwords, your personal information, your identity, and your money. This vulnerability is in large part an inherent consequence of the nature of the architecture that supports the Internet itself. It was not designed to be a fortress or to allow for the selective retention of safe spaces or neutral zones. For example, as Tony Townsend, information security analyst at the University of Virginia, argues: The Internet uses an antiquated design. Originally, there wasn't any thought of keeping people out—the Internet was designed to be open, to share data, to let people in. All of today's methods to prevent break-ins and keep the bad guys out have been added after the fact.*

This isn't a trivial concern. Enormous dollars and resources are at stake. Time spent trying to regain lost opportunities, damaged reputations, and heartache are real costs paid by the millions of victims of virtual crime, when intellectual property, identity, and livelihood are lost or threatened through the theft of proprietary data. The illegal acquisition and use of your personal information—social security number, credit card accounts, bank accounts, checking accounts, and passwords can fundamentally change your life in terrible, unrecoverable ways.

Criminals are waiting for you to make a mistake so they can get your password(s) when you inadvertently give them access. Criminals can get all of your passwords and access to all of your sensitive accounts when you install unwanted, hidden software (malware) on your computer, tablet, telephone, or other mobile device(s) that we increasingly take for granted as members of the information age. Criminals also attack from the other side of the virtual landscape, critically compromising the information technology, infrastructure, and systems of large corporations to steal their customers' critical financial data and access their personal records.

The financially devastating and widely publicized attack against mega-retailer Target in late 2013 leveraged both internal and external avenues of vulnerability. A phishing attack (discussed in Chapter 1) allowed the thieves to

access the credentials of a contractor working for Target. A poorly designed security infrastructure then allowed the credentials of that contractor, an HVAC company, to be used by the thieves to access the financial data of millions of customers, which they had no legal right to access.

It's not only criminals who are interested in getting their hands on your data. It is essential to not lose sight of the fact that larger, somewhat less ill-intentioned bodies also want access to your identity—at least parts of it. Your online identity is being constantly impinged upon, probed, evaluated, examined and recorded. This is being done not by criminals actively seeking to steal from you, but by bodies toward which we (at least some of us) ascribe relatively more benign intentions. Corporations and the government maintain an active, focused interest in you, your online persona, and what you do while you spend time connected to the Internet.

While corporations (hopefully!) aren't seeking to steal your password(s), they do want to know your spending habits—in detail, what other sites you are actively interested in, how much time you spend browsing, what clicks you make, and what keeps your eyes on one site vs. another. They are interested in your demographics and family information and your exercise, travel, recreational, interpersonal, and consumption patterns. They want to know all about you. They use the information they collect about you to directly micro-target their advertising specifically to you and more effectively set the hook for their own products and services—rather than those of competing firms also seeking your business.

The government also is very interested in you and what you are doing online. It wants to listen to your phone calls, to see what you have on your hard drive, and to monitor what you send over the Internet and Wi-Fi networks. It is interested in your e-mail, how you spend your money, where you travel, and who your friends are. Some of the surveillance that the government maintains is legal. Some is not. Many surveillance practices fall into a gray area, and their legality is being hotly debated, even today.

Although many of us would say that we have nothing to hide, some of the documents recently released by former US government contractor Edward Snowden—now living in Russia—are quite disturbing. For example, Snowden claimed in a July 2014 interview that National Security Agency (NSA) analysts routinely pass around the nude photos of innocent civilians intercepted by NSA operatives over the Internet. Access to these private, nude photos was considered a "perk" of the position according to Snowden and not seen in any way as a violation of civil liberties or an otherwise taken-for-granted right to privacy.[2] What remains is that, today, big brother really is watching and is

[2]Ars Technica, Cyrus Farivar, "Snowden: NSA Employees Routinely Pass Around Intercepted Nude Photos," http://arstechnica.com/tech-policy/2014/07/snowden-nsa-employees-routinely-pass-around-intercepted-nude-photos/, July 14, 2014.

paying very close attention to you and to what you're doing when you spend time online.

One of the emergent realities of the connectedness that defines our personal and professional lives today is that increasingly our "valuables," broadly defined, are not stored in physical locations or guarded by a lock and key. The most crucial strategic assets that banks hold are no longer stored in a giant safe in the basement with a combination lock and an armed security guard.

They are stored digitally in cloud space, protected by advanced mathematical fences and "impenetrable" dynamic algorithms. All "neighborhoods" are connected in the digital or online world. An axiom of the information age that we live in is that the openness that makes our immense progress possible also invites unwanted and unavoidable virtual proximity to real dangers. These dangers take the form of real criminals as well as overbearing intrusive authority and commercial interests that impinge on our treasure and personal liberties.

We're experiencing an ongoing, slow-moving shift of perception that also contributes to the dangers that users face. Today, although credit cards, PayPal, virtual money, check cards and other "clean" currency modalities (including the emergent Bitcoin, an entirely virtual and nationless currency) have become universal and ubiquitous, as a society we still retain an attachment (perhaps psychological, perhaps emotional) to thousands-of-years-old, archival, value transmission tools like the dirty coins and paper bills we carry around with us in our pockets.

As a society, we're still not comfortable with the redefinition of what is valuable today, or where this "value" resides. As an example, most of us would never take a wallet out of our pocket or purse and leave it on a conference room table or on someone's desk at the office while we run down the hall for 10 minutes. This would be crazy because there are valuables in that wallet—$89 in cash, a Visa, and a punch card to Yogurt Mountain that is one punch away from a freebie! Yet, in the modern American workplace an exact corollary of this unthinkable decision happens all of the time with smartphones, tablets, and laptops. In many ways the theft of one of these powerful data storage and delivery devices is likely to be significantly more financially consequential to the owner than the theft of his or her wallet.

In fact, more often than not the data stored on a digital device are significantly more valuable—and the costs of recovery significantly higher—than the device itself in which the data are stored. If an end user's laptop is stolen at the airport, the cost of the physical device (maybe $1,000 today) is likely covered by insurance, either personal or corporate, depending on who owns the device. Even if it's not covered by insurance, replacement is getting increasingly affordable. But the data stored on the device may take scores or hundreds of labor hours to re-create—or may even be completely unrecoverable. The theft also might lead to vulnerabilities in an organization's communications

infrastructure or networks, potentially exposing the personal and financial data of millions of customers, and costing millions and millions of dollars in recovery, damaged reputation, public relations rehabilitation, lost future business, and sunk resources.

The somewhat over-used term "hack," while still part of our popular vernacular, has recently been supplemented by a new, more accurate descriptor: the "Advanced Persistent Threat," or APT. While the term "hack" brings to mind a single action taken at a specific time, APTs are, as the name suggests, advanced and persistent. They're always out there. The attackers may take weeks or months to develop their assault, tracking the organization's behavior and IT infrastructure, probing for weaknesses, and developing the most effective way to attack.

Modern users can't simply secure their devices and watch their behavior at only certain times, or in certain places. APTs are constant and adaptable, and the vigilance of those potentially vulnerable to these modern attacks must be constant and adaptable as well (see Figure 1).

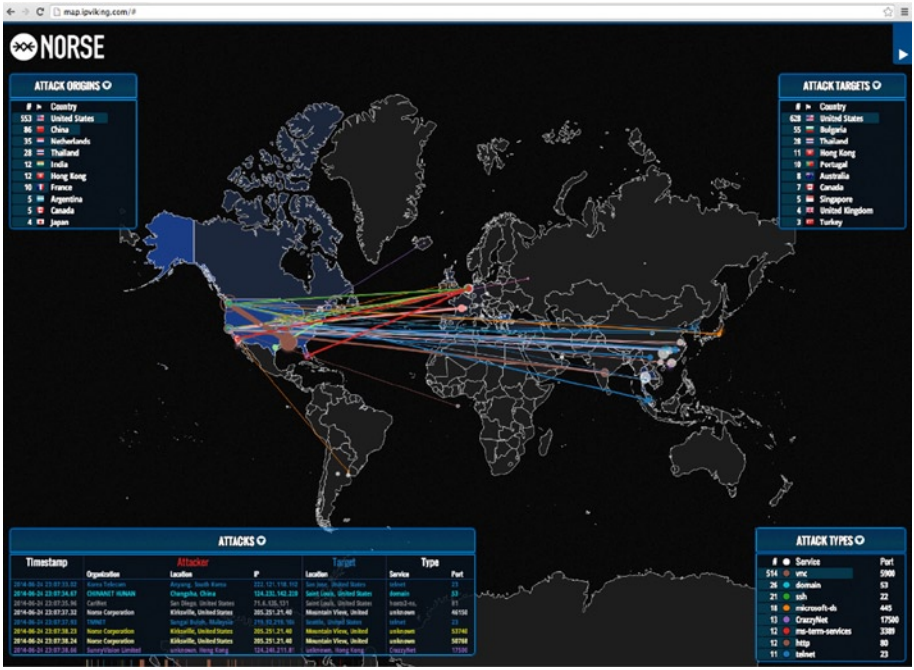

Figure 1. This live map, produced by the Norse Corporation, shows a real-time view of the origins and targets of digital attackers worldwide. (map.ipviking.com, used with permission)

The Internet that we all use, and increasingly take for granted as a functioning reality of our professional and personal lives, is in actuality an interconnected

global network—which is simultaneously both a really wonderful place and a really dangerous place. Because it provides us with the immediate access to data that we rely on in so many fundamental ways, it also puts our own personal data at risk. So, given that we can't pick and do not get to choose who comes into and out of our virtual neighborhood, what can we do? Although this is a frightening scenario, and the threat is real, there are ways to protect yourself against these evolving, ever-present dangers. In this book, we address approaches that users can adopt to minimize modern virtual threats.

The passwords that you use to limit access to your intellectual property and to your sensitive online accounts can slow criminals down. Choose them wisely, use them, protect them, and change them if they've been compromised. Follow the advice of experts. Communications from your corporate IT department and official e-mails from merchants with whom you trade should not be spammed or ignored. When they advise you to create a stronger password or to change your password, listen!

Lock your digital "property" up by protecting it with passwords that limit access to it. How do you keep your important property safe? What can you do? Some of these steps may have occurred to you, but others may be less obvious. Don't use an unsafe computer or public network to do private tasks like online banking. Obvious? Not necessarily. A lot of us like to work at the coffee shop, or get a few minutes of work done at the airport. Don't use ancient (here, read more than a couple of years old), unsupported devices. The technology in newer devices offers more sophisticated protection against intrusions that weren't in existence when previous generations of machines were designed and produced. Don't use outdated operating systems or programs. As these tools erode relative to the context in which they're embedded, thieves can take advantage of emerging security cracks.

The capabilities associated with, and our use of, the Internet are changing in such fundamental ways that many of us today don't really even understand where we store the important documents and data that we use. As a consequence, concerns and even genuine fear about online data storage (i.e., "in the cloud") have begun to pervade popular culture. This kind of reaction is common when new tools and approaches are widely and quickly adopted while a majority of the people who use the tool or adopt the approach don't really understand its strengths or limitations.

In the summer of 2014, Sony Pictures released the film Sex Tape, in which Jason Segel and Cameron Diaz play a married couple who accidentally store an intimate video of themselves on a public cloud location. Although the technical details portrayed in the film aren't 100 percent accurate, it plays on the average computer user's ignorance (and fear) of the cloud. As Segel's character exclaims in rage, "No one understands the cloud. It's an f-ing mystery!" Yet, despite our uncertainties about what the cloud is, and the implications of its use, there are safe (perhaps *safer* is a more appropriate

term here) ways to use cloud storage and cloud application providers, which we discuss in detail in the following chapters.

Keep your computer up-to-date and use antivirus software. Even if you run a firewall, if you let your protection get outdated, newer threats will be more likely to escape the protective net it offers. Don't try to use an old, outdated operating system (e.g., Windows XP) or an ancient phone or tablet. Here, "ancient" is broadly defined as any mobile device older than two or three years. The protections available through modern operating systems are essential to keep criminals from encroaching on your data today, but this has not always been so.

Don't give strangers access to your private financial data. Be very careful whom you allow to access your accounts and files. When non-family members have access to your home, your wireless network, or your devices, take precautions to protect yourself against unauthorized access to your data. We focus on some of these precautions in the chapters of this book.

Take prudent, informed steps to protect your most sensitive data from the scrutiny of corporations and government entities that operate with their own agenda in focus. Don't give commercial organizations access to or allow the government to access your Internet search history or activities online. What can you do to avoid this kind of snooping? Keep reading.

When traveling—for business or pleasure—take extra precautions to keep your data safe. Airports and hotels are very popular target sites for the physical theft of digital devices. Open Wi-Fi networks in airports, convention centers, and coffee shops can easily be hacked. Don't transmit sensitive data over any wireless network that doesn't require a password. Avoid using hotel business center computers whenever it's possible to do so—who knows if the last person to use that computer was a hacker! Turn off the Bluetooth on your phone if you don't need it, and don't let a stranger at the airport use your phone or computer. What can you do to increase the physical security of your devices at home, at work, and in transit? We discuss these issues in detail in Chapter 10.

Don't go into dangerous sites on the Internet. Don't try to get music, movies, or software for free on sites where these kinds of giveaways are advertised. More often than not—way more often than not—there's no free lunch when it comes to software or other applications. The much greater likelihood is that by visiting a tempting site that advertises freebies you will only make yourself vulnerable to infection and heartache.

If it seems like it's too good to be true—just like the drop-the-fat-pills that don't work and the knives that allegedly never get dull—it probably is. More than likely, the supposedly "free" stuff is going to come packaged with a virus or other malware that will dig right into your computer and open the

door for criminals to access your personal data. Develop a healthy sense of paranoia and skepticism when it comes to your data.

Why do criminals want your virtual property? There is big money—*big* money in identity theft. This is among the fastest growing crimes in terms of damages, a $375 billion-a-year crime that affects one in 25 Americans every year. Of course, not all of this identity theft is limited to crimes occurring over the Internet or in digital contexts.

People do still steal credit card statements from mailboxes, but the per capita incidence of digital crimes is on the rise, and it is increasing every year. Unwanted software, or what is referred to in technical circles as malware, is sometimes just written to cause havoc and is essentially an act of cyber vandalism, but far more frequently these programs are intended to generate profits for the criminals who write and deploy them. And they do—enormous profits.

So, how do criminals get your property anyway? There is never going to be a 100 percent secure fix or an absolutely airtight solution to the problem of unwanted intrusion or theft of your property. If a criminal is determined enough, he'll eventually break in one way or another. In reality you take security precautions so that the potential risks associated with theft of your property outweigh the potential rewards, so that the thief chooses another potential target.

It's not ultimately the integrity of a security system that serves as a deterrent to thieves trying to steal your property, but the potential costs of doing so that keep your property from being stolen. This is the same with all of the digital property that you'd like to keep safe. If you don't make it easy for criminals to get access to your private data, the cyber thieves who'd otherwise steal from you will move on to easier targets who've not protected themselves adequately. We'll show you how to keep your data safe.

The simplest way for thieves to get access to your property is by you making it easy for them. Your digital property is more likely to be stolen if you make mistakes like these:

- Your password is the word "password" or the digits "123" or your first name, etc.
- You leave your computer, phone, or tablet unattended at a coffee shop, or open and available when other people are in your home.
- You click links in an e-mail indiscriminately, without stopping to think (or find out) if they are legitimate.

- You store data indiscriminately in "the cloud" without considering the ramifications of doing so and/or the policies of your workplace.
- You don't change your password even after you think someone else might have learned it.
- You ignore warnings from corporate or consumer IT professionals concerning password strength, reuse, and retirement.
- You don't have a pass-code on your smartphone, even though you keep a list of account numbers or passwords on it.
- You connect to open, public Wi-Fi networks and transmit sensitive data over these unsecured channels.
- You visit "bad neighborhoods" on the Web, entering your e-mail address, password, and other private information in an effort to get free software, music, or movies.
- You use an ancient computer without updating your operating system or software applications.

More often than not people don't maintain even the most remedial precautions protecting their virtual property. You'd be surprised at the kinds of mistakes that otherwise well-informed, intelligent, professionals make when it comes to protecting their data from theft. Thieves will still try to trick you into letting them in even if you've got security in place. Unfortunately, end users fall for these tricks all the time. Thieves use the Trojan horse approach as it pertains to your digital property. Criminals may call on the phone and try to get your password by pretending to be someone authorized to have access to your information, someone you trust, like a network administrator or a company representative. Maybe they'll send you a "phishing" e-mail, trying to get you to click on a link that looks legitimate, and then provide your password or other personal information to a third party who will sell it or use it themselves. Maybe they have a free, open wireless network in a public place. Of course free public Wi-Fi is convenient, but are thieves stealing your data while you're using their air? Maybe they'll have a free app for your smartphone or tablet that makes wonderful claims—but is it stealing your data instead? We discuss these issues in depth in the pages that follow.

Successful criminals are clever, and they're getting more so all the time. When one avenue for theft or fraud is blocked, they'll find others. Just as nature builds a better mouse to avoid mousetraps, the approaches that criminals employ are also constantly evolving in the face of responses to the threat posed by their criminal activities.

Phishers and other data scammers will prey on human nature, using a psychological strategy called "social engineering." They'll attempt to learn more and more about their targets before making contact, increasing their odds of hooking an unsuspecting phish. They'll take advantage of human nature and our inclination to be kind, pretending to need assistance or adopting other approaches to gain sympathy and encourage potential victims to make themselves vulnerable to attack. They might also impersonate a person of authority, demanding access or the entering of a password, preying on our tendency to follow the rules and to respect authority. They'll often hint or explicitly state that their request bears on a critical, time-sensitive issue, giving the targeted victim no time to think. They'll use every trick in the book to get you to do what they ask.

In the end, it is critical to be very suspicious of people seeking access your data. Obviously, not everyone on the Internet is a criminal interested in stealing from you. But, the criminals are out there and it's best to be prepared. In this book, we develop a straightforward, linear approach for doing just that. We hope you find what follows to be useful to you as an informed, connected, active citizen of the 21st century.

CHAPTER

1

Don't Get Phished

Stay Out of the Net

Joe is a midlevel procurement manager with 14 years of experience at the multinational company Worldwide, Inc. His section is a large one, and much of the procedural updating that regularly comes through official channels is disseminated virtually—by text, the corporate instant messaging application, or e-mail. Joe rarely sees his immediate supervisor during the course of an average day and is accustomed to getting—and following—electronically delivered policy and housekeeping directives. Joe's communications with administrators from other sections in his division also typically come through company e-mail. From time to time updates to the company's IT systems require him to change his existing passwords or create new ones, so he is not uneasy when he receives a routine e-mail from his company's IT group directing him to update his system password (see Figure 1-1).

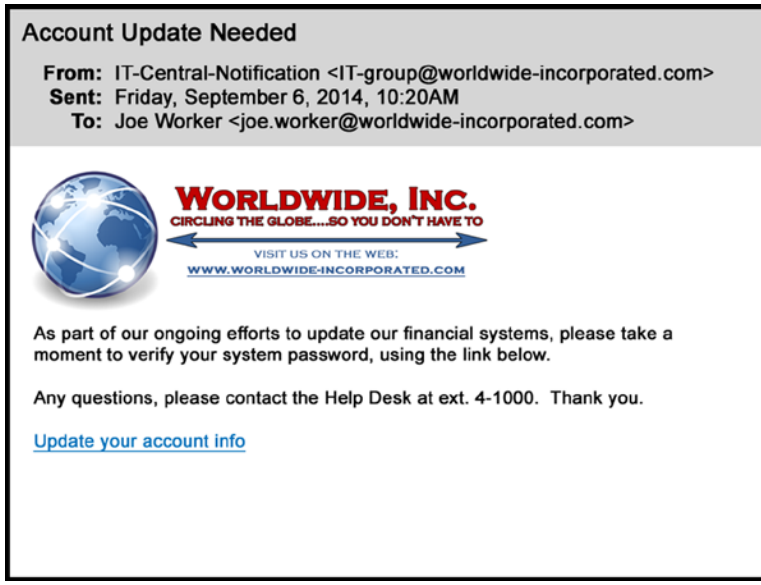

Figure 1-1. Sample e-mail asking for password confirmation and featuring two hyperlinks: the company logo and the "Update your account info" line

The e-mail is fairly well-written and looks kosher. It employs quasi-proper English grammar, incorporates the company logo in the usual way, and is signed with the correct phone extension for the IT help desk. The message contains a hyperlink to the company's web site and another for Joe to confirm his existing password and set a new one.

Joe nearly clicks the second link but hesitates when he remembers that upcoming system password changes are announced at the weekly section meeting and that he can't recall such an announcement having been made at the last one. He hovers his cursor over the hyperlink and is alarmed to see that it would take him not to his company's domain (Figure 1-2) but to a malicious domain (Figure 1-3).

Figure 1-2. Joe hovers his cursor over the account update hyperlink, expecting it to give his company's domain name, as shown

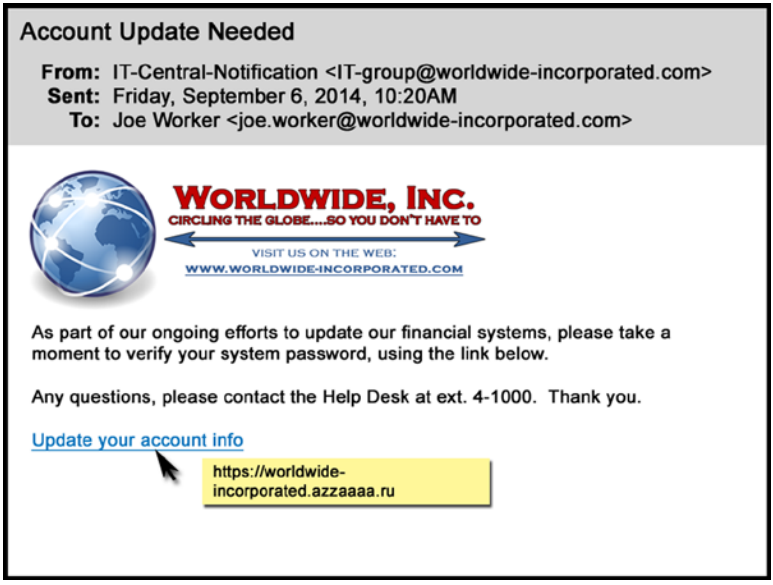

Figure 1-3. Joe instead sees that the hyperlink would take him to a malicious domain

A Closer Look at "Phishing"

"Phishing" is a virtual attack that uses a more or less compelling or attractive lure to acquire confidential or proprietary information through the use of fraudulent electronic communication. Victims of phishing attacks get caught when they take the bait offered by a phisher, such as an apparently legitimate request by their IT department to change a password or by their credit card company to protect an account with an additional personal information gate. E-mail is the most commonly used approach to launch a phishing attack, but such attacks can also be launched through web sites, text messages, IM (instant messaging), and mobile apps. Phishing techniques began to be deployed in the late 1980s, some years before the term itself was coined. The term derives from "fishing" for gullible users' login credentials and personal details, orthographically tweaked by substituting *f* with *ph* by analogy with "phreaking" (the practice of cracking phone network security to make free long-distance calls). The phish most commonly seen by IT departments is the one that almost snared Joe in the opening scenario. An electronic communication is sent to a target with a link embedded in a message that looks official but in reality originates from a fraudulent party seeking to steal personal information in order to gain malicious access or to resell to a criminal cyber organization.

Phishing techniques are increasingly sophisticated and well-crafted. No longer are incongruous language, improbable scenarios, or misaligned layouts used that give off the stink of phish that is immediately obvious to any employee. Today, the word choice, spelling, and grammar deployed in the most dangerous class of phishing messages are correct or, even better, are calibrated to be just slightly illiterate, in the same way that genuine corporate communications tend to be (as in Figure 1-1). Such phishes blend company logos, colors, design schemes, and other attributes of official communications in mimicry of legitimate messages that employees and customers routinely receive. Their sending e-mail addresses and hyperlink URLs are typically "spoofed" to resemble those of legitimate senders.

Sophisticated phishing operations are adept at securing and exploiting information about companies' internal changeover periods. If a company is in the process of undergoing IT system changes of any kind, its users are more likely to expect rather than suspect password change requests and other change-associated e-mails. Phishers prefer to time their attacks to correspond with periods of transition when users' psychological defenses are temporarily relaxed.

The majority of phishing attacks are *long-line* or *net phishing*. These attempts don't have a specific target. Their goal is to snare as many victims as possible following a volume or economies-of-scale approach and leveraging a broad, randomized targeting scheme. Contrasted with this kind of broadcast phishing