# FIGHTING PHISHING

## EVERYTHING YOU CAN DO TO FIGHT SOCIAL ENGINEERING AND PHISHING

ROGER A. GRIMES
WITH DR. JOHN N. JUST

WILEY

# Fighting Phishing

## Everything You Can Do to Fight Social Engineering and Phishing

**Roger A. Grimes**
**with Dr. John N. Just**

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394249206 (paperback), 9781394249220 (ePDF), 9781394249213 (ePub)



**Library of Congress Control Number:** 2023951446

Cover images: Hooks: © erhui1979/Getty Images
Background: © Vitalii Pasichnyk/Getty Images
Cover design: Wiley

*This book is dedicated to my wife, Tricia. We've been married for almost 25 years now. She's still my best friend and the one I want to be with every day. I've tried to be a better man since the day I met her.*

# Contents

# Introduction

Social engineering has been around since the beginning of humanity, and phishing has been around at least since the beginning of networked computers. I can remember my first brush with social engineering via computers in 1987. This was before most people had even heard of something called the Internet and before most people had personal computers. Many of us early adopters were on a precursor of the Internet called the FIDONet. Back in those days, you would use a 300 or 1200 BAUD or BPS (Bits Per Second) dial-up analog modem to call your local BBS (Bulletin Board System). This system would use a crude "store-and-forward" technology that would transmit and receive messages and files around the world in a day or so. We thought it all was pretty cutting-edge.

On one of the BBSs, I came across a downloadable text file named "How to Get a Free HST Modem." HST modems, made by US Robotics, were the fastest and best modems available at the time. They ran at an incredible 9600 BPS. They were expensive enough that only a few lucky, monied, people had them. They were mostly only used by Fortune 500 companies and well-funded universities. This file promised to tell anyone who read it how to obtain a free one. It was too enticing to pass up.

I opened up the file and inside it contained only text that said, "Steal One!" "Well, that was disappointing!," I thought. Then

the very next keyboard key I pressed formatted (i.e., permanently erased) my hard drive and rendered my computer useless. Well, at least until I reinstalled the operating system and redid everything all over again. I lost all files.

It turns out the file was something called an "ansi-bomb." It was a malicious file that took advantage of a feature of a legitimate operating system file called ansi.sys. Ansi.sys was a part of Microsoft's DOS operating system, which most of us ran at the time. Ansi.sys was an optional file that allowed users to have extended, "cool," features for their screen and keyboard, such as displaying special graphics and characters on your screen. It also allowed savvy users to map sequences of commands to a single key on their keyboard. It was meant to allow people to create "macros"—an automated shortcut that triggered a longer sequence of key presses. You could hit one or two keys and automate what would otherwise be a bunch of other key presses. Some malicious jerk had created a malicious file that instructed ansi.sys to map all the keys on the user's keyboard to format the user's hard drive when the next key was pressed.

It was a lesson learned.

There are malicious people in the world who want to harm other innocent people for no other reason than they can. Not everyone in the world is friendly and helpful, especially to strangers.

Now, the impact of social engineering and phishing on cybercrime has been driven home to me tens of thousands of times during my career. Today, nearly everyone understands that social engineering and phishing are responsible for more cybercrime than any other single initial root cause method. No other root cause of hacking is even close. But just a decade ago, even though it was true then, it wasn't as well known by all cybersecurity defenders. I think everyone knew social engineering and phishing was a problem, but few knew exactly how big of a problem it was. Few defenders knew it was the number one problem by far. Even I didn't.

I worked as a Principal Security Architect for Microsoft Corporation for nearly 11 years, from 2007 to 2018. For much of that time, I did security reviews for customers and installed Public Key Infrastructures (PKI) and advanced security defense systems. I was promoted, usually well-liked by clients, and always installed systems on time and on budget, which isn't so normal in the computer industry. For years I felt like I was greatly helping to protect my customers.

Then I realized that *every single* customer I had, no matter what defenses we installed, was still falling prey to hackers and malware. This was despite installing the best computer security defense systems possible. Why? It was almost always due to social engineering (and, secondarily, unpatched software). Even though all my customers were spending hundreds of thousands to millions of dollars to protect themselves using the most advanced systems the industry could imagine and deliver, what was taking them down was the same things that were most often taking down companies since the beginning of computers—social engineering. And usually, phishing.

That realization occurred to me in about 2016. It made me depressed. Instead of seeing myself as part of the solution, I realized I wasn't really helping my clients to avoid hackers and malware. What I was doing was more smoke and mirrors. I was wasting their time and money. But it wasn't like I was alone. Most computer security companies and consultants did what I did, which was concentrating on everything but defeating social engineering and phishing, even though they were clearly the biggest problem by far. Still, it bothered me tremendously.

I eventually wrote the first edition of a book about my realization, *A Data-Driven Defense: A Way to Improve Any Computer Defense* (`www.amazon.com/Data-Driven-Computer-Defense-Should-Using/dp/B0BR9KS3ZF`) in 2018. The book sold over 50,000 copies (over three editions), and its

premise—social engineering is most companies' biggest cybersecurity threat—led me to work for my current employer, KnowBe4.

The CEO of KnowBe4, Stu Sjouwerman, was one of the first people to read my book and understood its value in not only recognizing the importance of fighting phishing and social engineering but also in creating an effective cybersecurity defense using data. In April 2018, Stu offered me a job and I accepted. I was delighted. Not only was I going to start working for a leading firm in security awareness training, which is one of the best ways to fight social engineering and phishing, but I was also going to be able to concentrate on helping customers fight the biggest weakness in their cybersecurity defense as my primary job. I was pretty elated and remain so to this day.

In the over five years since, as KnowBe4's Data-Driven Defense Evangelist, I have taught hundreds of in-person presentations and online webinars. You can see many of my webinars here: `www.knowbe4.com/webinar-library`. You can download and read many of my whitepapers here: `www.knowbe4.com/security-awareness-whitepapers`. And you can request that I do a presentation to your company here: `www.knowbe4.com/security-awareness-training-advocates`. You can see dozens of my presentations for free on YouTube. I speak about a lot of topics beyond social engineering, including multifactor authentication, quantum, ransomware, passwords, password managers, nation-state hacking, and cryptocurrencies, but most of my presentations include something about fighting social engineering and phishing even if that isn't the primary topic. I never miss a chance to educate listeners about the importance of focusing on preventing social engineering and phishing.

There is nothing else most organizations could do better to reduce their existing cybersecurity risk than to reduce social engineering and phishing threats. This book is the best advice for today's world to help you fight social engineering and

phishing. I don't know of another source that has more coverage and suggestions. Not humbly, I think I can best teach anyone how to reduce their social engineering and social engineering risk. I break down many of the necessary critical lessons and processes into the simplest recommendations and charts you'll see anywhere. I cover every policy, technical defense, and best practice education practice you should be doing to best stop social engineering and phishing.

Do you want to know how to best reduce cybersecurity risk from social engineering and phishing? Read this book.

## Who This Book Is For

This book is for anyone interested in fighting social engineering and phishing attacks—from entire organizations to single individuals, from dedicated anti-phishing employees to IT managers, and for any IT security practitioner. Because the book contains large, distinct, sections dedicated to policy and formal security awareness training programs, it can be argued that it is more appropriately focused on organizations, ranging in size from small businesses to the Fortune 500. But individuals and organizations of any size will benefit from learning the recommendations and best practices contained in this book. Many of the lessons in this book should be shared with friends and family, and many of them are universal. This is the book I wish I read when I first got into the industry.

## What Is Covered in This Book

*Fighting Phishing: Everything You Need to Know to Fight Social Engineering and Phishing* contains 17 chapters separated into 4 parts.

- **Part I: "Introduction to Social Engineering Security."** Part I will begin by introducing all the data and terminology

associated with social engineering and phishing. There are dozens of distinct definitions that will help you better understand and talk about social engineering and phishing. Part I ends with a discussion about the three necessary components needed in any computer security defense, including one that fights social engineering and phishing.

- **Chapter 1: "Introduction to Social Engineering and Phishing."** Chapter 1 discusses the data and facts around social engineering and phishing and why it is so important to defeat if you want to defeat hackers and malware. If you need to prove to management the importance of fighting social engineering and phishing in your organization, this chapter will help you deliver that argument.
- **Chapter 2: "Phishing Terminology and Examples."** Chapter 2 describes the dozens of definitions related to social engineering and phishing. There are many different types of social engineering and phishing, and understanding the differences will help you better understand the threat and how to best fight it. Different types of social engineering and phishing require different types of defenses. Many different examples of phishing attacks will be presented.
- **Chapter 3: "3x3 Cybersecurity Control Pillars."** All security defenses require a best risk-managed, defense-in-depth, combination of policies, technical defenses, and education to best fight cyber threats. Chapter 3 covers compliance, risk management, defense-in-depth, and the three defensive pillars all defenders must know and deploy to fight hackers and malware, not just against social engineering, but any cyber threat.

- **Part II: Policies.** "Part II discusses all the general and specific policies that any organization should create and deploy to help fight social engineering and phishing.

- **Chapter 4: "Acceptable Use and General Cybersecurity Policies."** Chapter 4 covers general Acceptable Use Policies and general cybersecurity policies that every organization should create and deploy to minimize cybersecurity risk. As part of the cybersecurity policy section, many general best practice security recommendations will be covered. Cybersecurity education begins with good policies and this chapter begins that educational process.
- **Chapter 5: "Anti-Phishing Policies."** Chapter 5 covers all the specific policies that every organization needs to create and deploy to minimize social engineering and phishing.
- **Chapter 6: "Creating a Corporate SAT Policy."** Chapter 6 is for larger organizations that require an official security awareness training program policy. It covers all the components a security awareness training policy should contain and finishes with an example policy that can be used by readers to create their own.

- **Part III: "Technical Defenses."** Part III covers all the software and hardware tools that someone can utilize to minimize social engineering and phishing attacks.
  - **Chapter 7: "DMARC, SPF, and DKIM."** Chapter 7 covers the Domain-Based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) anti-phishing standards and how to deploy them within your environment.
  - **Chapter 8: "Network and Server Defenses."** Chapter 8 covers the most common types of network-deployed and server-level cyber defenses used to fight social engineering and malware threats. It includes content-filtering firewalls and gateways, anti-phishing filters, and network connection mapping.

- **Chapter 9: "Endpoint Defenses."** Chapter 9 covers the most common endpoint-deployed cyber defenses used to fight social engineering and malware. It includes anti-malware scanners, endpoint detection and response software, content filters, browser defenses, and email protections.
- **Chapter 10: "Advance Defenses."** Chapter 10 covers advanced defenses like using separate "red/green" systems, hypervisor-hardware-enforced isolation systems, DNS defenses, and sophisticated malware detection defenses.

- **Part IV: "Creating a Great Security Awareness Training Program."** One of the most neglected parts of fighting social engineering and phishing is creating a GREAT security awareness training program. The last part of this book is dedicated to telling anyone how they can create a GREAT security awareness training program. If you follow what this section contains, you can help significantly reduce cybersecurity risk in your organization.
  - **Chapter 11: "Security Awareness Training Overview."** Chapter 11 gives a broad overview of how to create a sophisticated security awareness training program, including what it should contain, who should be involved, and what tools and methods should be used. If you want to know how to set up a *great* security training program, begin here.
  - **Chapter 12: "How to Do Training Right."** Great training doesn't just happen. It takes planning, preparation, logistics, and cooperation. Written by Dr. John Just, Chapter 12 covers the types and quality of training that all *great* security awareness training programs should have including quizzing, next steps, and quality feedback loops.

- **Chapter 13: "Recognizing Rogue URLs."** One of the best skills you can give anyone is how to recognize a phishing URL. Chapter 13 covers, in detail, how anyone can tell the difference between legitimate and rogue URLs. It includes dozens of examples of rogue URLs and how anyone can detect the fraudulent aspects.
- **Chapter 14: "Fighting Spear Phishing."** Spear phishing is responsible for more successful data breaches than any other single threat and takes specific training to defeat. Chapter 14 discusses how you need to modify your "regular" security awareness training program to address the very real risk of spear phishing.
- **Chapter 15: "Forensically Examining Emails."** Chapter 15 covers how to forensically examine any email to better determine if what you are looking at is a phishing email or not. It covers dozens of methods, including DMARC, reverse DNS lookups, domain name investigating, blocklisting, and physical address locating. If you have ever been stumped on whether an email you are looking at is a phishing email or not, this chapter is for you.
- **Chapter 16: "Miscellaneous Hints and Tricks."** Chapter 16 covers suggestions and hints that didn't fit in other chapters, like strict anti-phishing policies, text-only emails, SAT counseling, and more.
- **Chapter 17: "Improving Your Security Culture."** The Holy Grail in the computer security defense community is to create a lasting culture of pervasive cybersecurity in the organization so that everyone practices excellent cyber hygiene resulting in a significant reduction in organizational cybersecurity risk. Chapter 17 will define the components of a security culture and discuss how you can get your organization there.

All together, these 17 chapters and the lessons and best practice recommendations they contain should allow anyone to craft their best, most efficient plan in fighting social engineering and phishing. I've tried to put the best possible defenses and best practice recommendations about fighting social engineering and phishing into this book. This should give you the techniques and tools to make your security stronger than ever. With that in mind, continue to fight the good fight!

## How to Contact Wiley or the Author

Wiley strives to keep you supplied with the latest tools and information you need for your work. Please check the website at `www.wiley.com/go/anti-phishing`, where I'll post additional content and updates that supplement this book should the need arise. If you have any questions, suggestions, or corrections, feel free to email me at `roger@banneretcs.com`.

PART

I

# Introduction to Social Engineering Security

Part I includes three chapters that set a basic understanding of social engineering and phishing threats and finishes with the beginnings of what it takes to create a great defense-in-depth defense. Chapter 1 discusses social engineering and phishing and why you need to defeat them if you are to have a successful defense. Chapter 2 covers phishing terminology along with many real-world examples. Chapter 3 discusses the 3x3 Cybersecurity Control Pillars and how every security defense must have policies, technical components, and education to be successful.

CHAPTER

# 1

# Introduction to Social Engineering and Phishing

Chapter 1 is going to discuss the importance of fighting social engineering and phishing. If you have to persuade your boss or colleagues why fighting against these threats matters, this chapter is for you.

## What Are Social Engineering and Phishing?

I think everyone knows what phishing is. It's hard to go an entire day without being exposed to it in some way. It's everywhere! We know it when we see it. Most of us are exposed to it daily, or nearly daily, usually through scam emails, text messages, or calls to our cell phones. Figure 1-1 shows a representative common example of a phishing email.

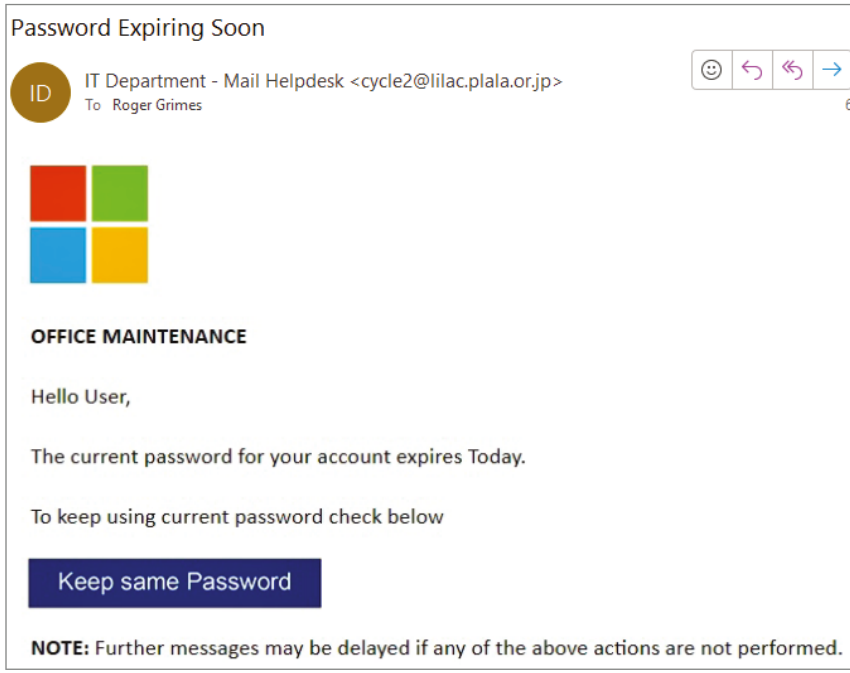


**FIGURE 1-1** Common type of phishing email.

Figure 1-1 is an example of a very common type of phishing email, likely the most common, where the phisher is attempting to make it look like an official email from Microsoft asking for an account password. If a victim were to click on the "Keep same Password" button, they would be directed to a fake, look-alike website asking for the victim to input their real account password. There are many classic signs of this being a phishing email, which we will be discussing in more detail in future chapters, but the most obvious is that the originating email address comes from some random email address from Japan (as indicated by the domain suffix of .jp) and is not `microsoft.com` as would be a real email from Microsoft.

Some people might wonder what's the difference between social engineering and phishing and why I call them out separately. *Social engineering* is a malicious fraud scam, where a

perpetrator often pretending to be someone else, a group, or a brand that a potential victim might implicitly trust more (than an unknown person) attempts to get the victim to perform an action that is contrary to the victim's self-interests. The perpetrator doesn't always have to be unknown. The scammer could be someone the victim knows or even knows well (like a best friend or family member). But in today's digital world, most online digital scams are committed by people we don't know.

Social engineering is as old as humanity. There are many ancient, early written examples of people complaining of scams and being taken advantage of. You can find an example of an early financial scam documented back in 300 B.C. at `www.investopedia.com/articles/financial-theory/09/history-of-fraud.asp`.

Social engineering is exploiting the inherent trust one human gives another. We are built to trust each other by default. In general, this default trust serves us well. Most of what we do every day only works because our default assumptions and inherent trust in other human beings work most of the time without harming our interests. Most of our civilization only works because that trust is usually well-founded most of the time. But scammers take advantage of this default trust.

Commonly, scams are done for monetary advantage, but they can be done for many other reasons, such as romance, revenge, jealousy, physical harm, and really in response to any emotion, even happiness. People often socially engineer friends and loved ones into situations that will benefit all those involved (for example, a surprise birthday party or giving rewards for a desired behavior). In the context of this book, however, we are talking about malicious social engineering scams that involve one party intentionally harming another.

There are a lot of ways for someone to be socially engineered and scammed. Basically, any communication method between two parties can be used for a scam, including in-person, physical

mail, phone calls, text messages, email, websites, instant messaging, collaboration apps, and social media. If there is a will there is a way to scam someone. It wouldn't surprise me to learn that various cultures throughout history scammed each other using carrier pigeons, semaphores, signal fires, or some other communication method.

*Phishing* is a type of criminal social engineering that involves online digital media. The most common form of phishing is done using email, but it can be done using any electronic communication channel, including websites, instant messaging, phone text messages, and even voice calls. I'll cover the different types of phishing in more detail in Chapter 2, "Phishing Terminology and Examples." You will hear some people calling all forms of social engineering phishing, and that's OK because we all understand what the person is communicating in the entire context. It doesn't make sense to get caught up in an argument about whether an analog phone call is phishing or not. It's all bad. But you should understand that social engineering is broader than phishing no matter how you define either term. This book is designed to help people avoid all malicious social engineering, but it naturally has a strong focus on phishing given today's online digital world.

There is a lot of social engineering and phishing going on. Millions of people and companies lose billions of dollars each year to scammers. Phishing, because it is digital, easily scales. It is low cost and low risk (the vast majority of phishing scammers get away with their crime, at least for some years), and it can be performed on tens of millions of potential victims a day by a single perpetrator. All the *phisher* (i.e., a person who originates or spreads a phishing message) needs is a valid email address, account name, website address, or phone number, for themselves and the potential victims. Usually, they can easily get potential victim contact addresses in the many millions at one time.