

MAX PARADOX

PROBLEM? RELAX. YOU'VE GOT THIS!

Self-Help with a Sense of Humor ;)

Every Message Looks Like a Scam

How to Stay Safe Online Without Suspecting Your Own Grandma



We have a problem. Relax. We can solve it—and have a laugh along the way.

TABLE OF CONTENTS

INTRO	1
Chapter 1 - Why Everything Suddenly Looks Suspicious.....	9
Chapter 2 - The Message Wants You to Hurry	22
Chapter 3 - The Clues You Trust Too Much	36
Chapter 4 - You Can Be Too Suspicious.....	49
Chapter 5 - Stop Clicking to Find Out.....	62
Chapter 6 - Your Inbox Is Not Your Boss	75
Chapter 7 - Politeness Is Expensive	91
Chapter 8 - Stop Memorizing Scams	103
Chapter 9 - Use Another Door.....	117
Chapter 10 - The Five-Minute Verification Routine	131
Chapter 11 - Codes Are Not Conversation.....	146
Chapter 12 - Money Makes Messages Dangerous.....	159
Chapter 13 - When the Message Sounds Exactly Like Them	175
Chapter 14 - Nobody Needs to Control Your Screen	189
Chapter 15 - What If You Already Started?.....	202
Chapter 16 - When You Cannot Verify Anything	216
Chapter 17 - The Day You Stop Being Careful	231
Chapter 18 - Notice When the Old Problem Comes Back .	244
Chapter 19 - Build a System That Does Not Need You to Be Brilliant.....	258
Chapter 20 - Safe Enough to Live Normally	270

INTRO

Your phone buzzes.

"Hi! Your package could not be delivered. Please confirm your address here."

You stare at the message.

You are, in fact, waiting for a package.

Suspicious.

You look at the sender. Some random number. Very suspicious. The link contains the name of a delivery company, except there is an extra letter hiding in the middle like a criminal wearing a fake mustache. Extremely suspicious.

You delete the message.

Thirty seconds later another one arrives.

"Hey, it's Mom. I changed my number."

Now we have a situation.

You call your mother. Her phone rings on the kitchen counter while she answers your call from exactly the same number she has had since approximately the invention of electricity.

Scam.

Excellent. You have successfully defended the perimeter.

Then your bank emails you about a new statement. Scam? Your streaming service says your payment method expires next month. Scam? A coworker sends you a shared document. Scam? Your cousin messages, "Look at this photo of you." Absolutely scam. Nobody has ever introduced a photograph with words that reassuring.

At some point, online safety stops feeling like safety and starts feeling like living in a small digital bunker where every notification is examined under a lamp.

"Who sent you?"

"Why are you here?"

"Where were you on Tuesday?"

The message would like to remind you that your dentist appointment is at 3:30.

This is the strange problem we have created for ourselves. Online scams really are everywhere. Phishing emails, fake delivery notices, account alerts, cloned websites, impersonation messages, fake invoices, romance scams, marketplace scams, investment nonsense, support-agent impersonators, and urgent messages from people who have apparently changed both their phone number and personality overnight.

Being cautious is rational.

Being suspicious of literally everything is exhausting.

And unfortunately, the internet does not provide a neat visual distinction. Legitimate messages do not arrive wearing a white hat while scams enter accompanied by sinister violin music. Sometimes the fake message looks polished, professional, and perfectly ordinary. Sometimes the real message looks like it was written in a basement during a power outage.

This is inconvenient.

A genuine bank email may contain awkward wording. A real delivery company may use a link you do not recognize. Your actual employer may send a terrible-looking automated login notification. Meanwhile, a scammer can copy logos, colors,

formatting, names, and language so well that the message looks more professional than the company it is impersonating.

The old advice—"just look for spelling mistakes"—has aged about as well as "never get into a stranger's car," now that millions of people routinely summon strangers in cars using an app.

The problem is not that you are foolish. The problem is that you are being asked to make dozens of tiny trust decisions in an environment specifically designed to make those decisions difficult.

You receive a message. You have three seconds before curiosity, fear, urgency, greed, politeness, or habit takes over.

"Your account will be suspended."

Click.

"Someone tried to log in."

Click.

"You have an unpaid toll."

Click.

"Your refund is waiting."

Click.

"Is this you in this video?"

Click.

Congratulations. Your nervous system is now operating customer support for the entire internet.

Scammers understand something important about human beings: we are much easier to manipulate when we are rushed. A message does not need to convince you for twenty minutes. It only needs to make clicking feel slightly easier than thinking.

That is why so many scams contain urgency. Pay now. Verify now. Respond immediately. Your account is at risk. Your package is disappearing into a mysterious postal dimension. Your boss needs gift cards before lunch for reasons that will definitely survive a reasonable follow-up question.

Urgency narrows attention. Fear makes us want certainty. Familiar names lower our guard. Small amounts feel harmless. Authority makes us hesitate to challenge the request.

And sometimes politeness finishes the job.

A stranger messages, "Sorry to bother you, is this Sarah?"

You are not Sarah.

A reasonable response would be to ignore it.

Instead, part of your brain says, Well, I should tell them. Otherwise they may spend the whole evening looking for Sarah.

Sarah will survive.

This book is not going to teach you that every unexpected message is dangerous. That approach technically reduces some risk in the same way never leaving your house reduces the risk of being hit by a bus. It also creates several new problems, including becoming the person who calls their bank to verify whether the bank's phone number is really the bank's phone number.

The goal is not maximum suspicion.

The goal is better verification.

Those are very different things.

Suspicion says, "Everything might be fake."

Verification says, "I do not need to guess."

That shift is the foundation of everything we are going to do.

You do not need to become a cybersecurity expert. You do not need to memorize fifty kinds of phishing attacks, inspect email headers for recreation, or spend your evenings studying domain registration records while your family quietly moves dinner to another room.

You need a small set of reliable habits that work even when the scam is convincing.

You need to know when not to click.

You need to know how to verify a message through a separate route instead of using the contact information the message conveniently provides.

You need to recognize the psychological buttons scammers press: urgency, fear, authority, curiosity, scarcity, embarrassment, and the powerful human desire to make an annoying notification disappear.

You need to know what to do when a message seems legitimate but something feels off.

And, importantly, you need to know what to do if you already clicked.

Because “never make a mistake” is not a safety strategy.

It is a fantasy written by someone who has never tried to use the internet while tired, distracted, carrying groceries, answering work messages, and wondering why the cat is making that noise.

We are going to build something more useful: a simple decision process that helps you separate normal communication from situations that deserve more checking. We will look at links, payments, passwords, one-time codes,

account warnings, family impersonation, fake support messages, marketplace conversations, suspicious calls, and the increasingly weird world of messages that may sound exactly like someone you know.

The aim is not to turn you into the digital equivalent of a border guard interrogating your grandmother because she sent "Happy birthday" without an emoji.

The aim is to make scams boring.

Not harmless. Not nonexistent.

Boring.

A suspicious message arrives. You know what to check. You check it. You verify through a trusted route when necessary. You continue with your day.

No panic.

No detective board with red string.

No forty-minute investigation into whether FedEx has secretly changed its logo.

You will still occasionally receive a message that makes you narrow your eyes at the screen.

Good.

A little caution is useful.

We are simply going to teach that caution some manners.

By the end of this book, you should not trust everything online. That would be a terrible outcome and possibly the shortest cybersecurity career in history.

You should know when trust is reasonable, when verification is necessary, what steps to take, and how to act without letting every text message trigger a small internal fraud investigation.

Your grandmother may still send unusual messages.

That does not automatically make her a cybercriminal.

Although if she asks for \$2,000 in cryptocurrency because she is "stuck at the airport," perhaps give Grandma a call.

Next input according to the master flow is simply continue.

Chapter 1 - Why Everything Suddenly Looks Suspicious

You open your inbox and see a message from a company you actually use.

"Your account requires attention."

Excellent.

Nothing improves a Tuesday morning like a vague digital threat.

You recognize the logo. The sender name looks right. The colors are right. There is even a polite footer explaining how seriously the company takes your security, which is comforting in roughly the same way as a restaurant displaying a large sign saying WE DEFINITELY WASH THE FORKS.

You hover over the button.

Maybe it is real.

Maybe it is fake.

Maybe clicking it will take you to your account.

Maybe clicking it will result in a man named Viktor buying three laptops with your credit card before you have finished your coffee.

So you close the email.

Then you reopen it.

Then you search the company name online.

Then you compare the sender address.

Then you search: "Is email from companyname-security-alert.com legit?"

Fifteen minutes later, you have found six forum discussions, three conflicting answers, an article from 2019, and one person on Reddit who appears convinced that the entire company is a front operated by an intelligence agency.

The email was real.

You have survived.

You have also spent fifteen minutes authenticating a notification about a \$9.99 subscription.

This is the first important thing to understand: when scams become common enough, the cost is not limited to people who get scammed. Everyone starts paying a smaller tax in attention.

Every message requires a tiny decision.

Safe or unsafe?

Real or fake?

Ignore or act?

Click or do not click?

That decision used to be mostly automatic. A friend sent you a link, so you opened it. Your bank contacted you, so you read the message. A retailer sent a receipt, so you glanced at it and moved on.

Now your brain has learned a new rule:

Unexpected communication may be hostile.

That rule is not irrational. It is simply incomplete.

If your only safety rule is “unexpected equals dangerous,” ordinary life becomes difficult very quickly. Doctors call unexpectedly. Delivery services text from unfamiliar numbers. Companies change email systems. Friends send