SAMPLE

The Fake Buyer

Anatomy of a Marketplace Phishing Scam — the S$1 Ebook, the Forged Receipt, the Test Card That Gave It All Away, and Every Trick in the

Aiman Sterling

Free sample: Introduction & Chapter 1

putrabooks.github.io

Contents

Introduction

Chapter 1: One Dollar, One Listing, One Badge

Chapter 2: The Email That Should Not Exist

Chapter 3: The Redirect

Chapter 4: The Receipt

Chapter 5: Four Two Four Two

Chapter 6: The Twelve-Hour Clock

Chapter 7: Technical Support

Chapter 8: The Three Endings

Chapter 9: Why the Marketplace Hides Your Email

Chapter 10: The Seller's Defense

Chapter 11: The Afterlife — Reporting, Records, and the Throwaway Address

Afterword: The One-Dollar Verdict

References

Appendix: The Pre-Incident Timeline

This free sample contains the Introduction and Chapter 1. The complete book contains the full contents above.

Introduction

This book is the complete record of one phishing attack, preserved from the moment it knocked to the moment it ran out of script. It happened on September 30, 2026, to a one-person publishing operation selling an ebook for one Singapore dollar on Carousell — and it failed, which is exactly why it can be documented so completely. The scammer lost nothing but time, the seller lost nothing but an evening, and the full exchange survives as a specimen: every message, every forged document, every pressure tactic, with timestamps.

There are books about fraud that describe the category. This one refuses that altitude. It stays at street level, in the order the attack actually unfolded, because the anatomy of a phishing scam is only visible in sequence. The first contact looks harmless. The second looks eager. The third carries a document that looks, at a glance, exactly like the marketplace's own paperwork. Each step is survivable alone; the scam is designed so that by the time the dangerous step arrives — the QR code, the twelve-hour deadline — the target has already agreed to the frame: a buyer exists, a payment exists, the only remaining question is how the seller completes the sale. Once that frame is accepted, every subsequent instruction feels like cooperation instead of attack.

The record starts with a red badge. A "1" on a marketplace account that had, at that point, no buyers, no sales, and no messages — and the hunt for the buyer behind the badge, which found an automated assistant instead. It continues with an email that should not have been able to exist: a stranger writing to the seller's private Gmail address about a listing that, by the platform's own design, does not display that address to anyone. Then the reply, the "payment," the receipt, the QR code, the deadline, the "Technical Support," and finally the strange, almost melancholy way the script repeated itself when nothing worked.

Along the way, the attack left fingerprints that are worth learning by name. A payment confirmation citing card ····4242 — the most famous test card number in the software industry, a number that cannot carry a real charge anywhere on Earth. A $4.99 shipping fee matching the listing's original, long-corrected price — the receipt describes a version of the listing the seller had already edited away, which is how a forgery dates its own scrape. A twelve-hour validity window on an invoice no real system issued. A scan instruction — "the digital code," your phone camera — in a document whose recovered original quietly confesses that the code area was an empty placeholder ("No image") while a look-alike button carried the real payload: the attack's front

door is whatever ships, which is why the defense aims at the pattern, not the door.

Every element is dissected in the chapters that follow: what it was, why it was built that way, what it was counting on the target not knowing, and what the correct counter-move was at each step. The book ends with the seller's defense as it actually worked that night — a platform audit, a receipt read forensically, a refusal to scan, and the discovery that a scam script, like a bad employee, has only one page and will read it to you twice.

The names are handled with care. The seller's identity, email, and account details are pseudonymized throughout. The scammer's address is preserved in the record where it matters as evidence, because it is a disposable artifact of the attack, not a person. The quotes are verbatim. The timestamps are real. The one dollar was never at risk for longer than it took to read a receipt.

That is the whole story. It is small — one ebook, one evening, one attacker. But phishing works at exactly this scale, one small seller at a time, and it is defeated at exactly this scale too, one receipt read carefully at a time. This book exists so that the next seller reads the receipt carefully.

Chapter 1: One Dollar, One Listing, One Badge

The item for sale was an ebook. A PDF, one dollar, listed on Carousell — the marketplace that runs Singapore's secondhand economy and, increasingly, its micro-scale digital goods. The listing was precise about what it was: a nonfiction investigation of a five-hundred-year-old Moroccan legend, delivered to the buyer through the platform's own chat once payment cleared. The description ended with the sentence that matters to this story: no physical item will be shipped. One dollar, one file, one chat. The smallest possible commercial unit the platform supports.

The seller behind it was a one-person publishing operation — the kind that researches, writes, edits, packages, and lists its own catalog — with an account that had been around for years but carried no sales history and no reviews. On the day of the attack, the listing had been live for under nine hours. It had zero likes, zero chats, and zero views worth mentioning. In the attention economy it was, at that moment, an object in the dark.

That is not a disclaimer. It is the point. Phishing at marketplace scale does not hunt the successful. It hunts the newly listed, the unrated, the one- dollar sellers — accounts that have no baseline of normal activity against which an anomaly would stand out. A seller with fifty completed transactions knows what a real order looks like because they have received fifty of them. A seller with zero completed transactions has never seen a real order, which makes them perfectly positioned to mistake a forged one for their first.

At 1:23 in the afternoon, the platform's automated assistant account — the official onboarding robot that messages every seller the first time they enable a feature — sent the account a chat:

> "Hey @seller, you just enabled the 'Buy' button on your listing for the first time! Do you know how you can get paid when a buyer purchase your listing via 'Buy' button?"

The seller had, indeed, just enabled the Buy button, the one-tap instant-purchase option that lets a buyer pay without negotiating. The badge on the account header changed from nothing to "1," exactly as it would if a buyer had made contact.

Read the assistant's message again with fresh eyes, because it is a piece of accidental camouflage. It mentions a buyer. It mentions payment. It mentions the listing. Delivered as an in-app notification on a phone, stripped of the sender's label, it occupies the same visual slot as "buyer is interested." The seller's first conclusion — that a buyer had appeared — was not careless. It

was the reasonable reading of a badge the platform assigns to an automated tip.

The hunt for the buyer began that evening. The inbox, opened in a full web session, contained three chats, every one of them official: the assistant's Buy-button tip from that afternoon, and two survey invitations from the platform's research account, from 2024 and 2025. The sales dashboard reported no active orders. The listing's own page — the definitive record, because it is where the platform keeps the state of the product — said "No chats yet."

An audit like this one has a shape worth remembering, because it is the same shape a fraud audit should always take: go to the primary system of record and enumerate everything. Not the notifications, which are interpretations of state; the state itself. The badge said one thing. The platform said another. The platform wins, and the discrepancy itself — badge without message — was the first diagnostic finding of the night, filed hours before the real attack arrived: something was generating buyer- shaped signals around this account without a buyer existing.

The badge was true in the narrowest sense: there was one unread chat. It belonged to the assistant. But the account had a second condition that made the signal worse than useless: the registered mobile number on the account was outdated and unreachable, so every SMS the platform had ever sent to it had been dying quietly for years. The account's notification surface, in other words, had decayed into a state where a badge could appear with no working channel to explain it — a phone that cannot receive codes, an email channel that does receive, and a chat system the seller did not habitually open on the web.

That decayed state is not unusual. It is the resting condition of millions of accounts: created years ago, phone number long since changed, email still live, notifications half-working. Phishing does not create this condition. It harvests it. The attack that follows in the next chapter did not need to guess that the seller's phone was dead; it needed only to route around the phone entirely and arrive in the one channel that worked — email — dressed as the platform.

The badge, then, played its role without ever intending to. It spent the evening training the seller to expect a buyer. When the buyer finally did arrive, by email, an hour before midnight, it arrived into a mind that had already done the believing. The scam did not have to convince the seller that a buyer existed. The assistant's badge, the dead phone, and an evening of searching had done that work in advance.

That is the first lesson of the record, and it costs the least to learn: an expectation is an attack surface. The badge created one; the email cashed it.

End of free sample. The full book is available at putrabooks.github.io