Solve your problem with a wink

I'm Selling a Sofa, So Why Does the Buyer Want My Card?

How to Buy and Sell Safely on Online Classifieds Platforms



Max Paradox

I'm Selling a Sofa, So Why Does the Buyer Want My Card?

How to Buy and Sell Safely on Online Classifieds Platforms

Max Paradox

PROBLEM? RELAX. YOU'VE GOT THIS!

ISBN: 9788384905906

ALL-IN Rafał Płonkowski



CONTENTS

INTRO 5

Chapter 1 - When an Ordinary Listing Turns Into a Trap 10

Chapter 2 - Why Does a Scammer Sound More Convincing Than Your Own Common Sense? 19

Chapter 3 - Seven Red Flags That Should Stop Your Transaction 29

Chapter 4 - The False Sense of Security: How We Make a Scammer's Job Easier 39

Chapter 5 - Not Every Bargain Is a Bargain: How to Shop Without Switching Off Your Common Sense 50

Chapter 6 - Sellers Need to Be Careful Too: How Not to Give Away Your Money Along With the Item 59

Chapter 7 - Safe Payments: Why Money Shouldn't Travel on Trust Alone 69

Chapter 8 - You Don't Have to Be Nice at Any Cost: The Art of Ending Suspicious Conversations 79

Chapter 9 - Keeping the Transaction Under Control: From the First Message to the Final Confirmation 91

Chapter 10 - A Digital Detective Without a Magnifying Glass: How to Check Information Before Believing a Listing 100

Chapter 11 - A Link to Your Money or a Link to Trouble? How to Recognise Fake Messages and Payment Websites 110

Chapter 12 - Your Account Isn't a Communal Cloakroom: How to Secure Access to Classifieds Platforms and Online Banking 119

Chapter 13 - The Parcel Arrived, but Reality Forgot the Description: How to Resolve Disputes After a Purchase.....128

Chapter 14 - Before the Scammer Disappears With Your Money: What to Do When a Suspicious Transaction Becomes a Real Threat.....139

Chapter 15 - When a Scam Has Several Layers: Difficult Cases Where Ordinary Caution Isn't Enough.....149

Chapter 16 - When Caution Loses to Real Life: What to Do When You Have No Time, Knowledge or Ideal Conditions.....160

Chapter 17 - I Fell for a Scam. Now What? How to Regain Control After the Damage Is Done.....171

Chapter 18 - Safe Shopping Without Everyday Paranoia: How to Maintain Good Habits 181

Chapter 19 - When Common Sense Goes on Holiday: How to Recognise the Return of Old Mistakes 192

Chapter 20 - Sell Your Sofa, Not Your Peace of Mind: How to Make Safe Decisions Independently..... 203

INTRO

You're putting your sofa up for sale. Photos taken, price reasonable, description honest. You've even arranged the cushions to make them look happier with life than you do on a Monday morning. Seven minutes later, a message arrives. The buyer is ready to go. No haggling, no questions about dimensions, no interest in the colour or the fact that the left armrest still remembers the previous owner. They want to buy it immediately. They have just one request: you need to click the link they've sent, enter your card details and confirm receipt of the money.

Interesting. You're selling a sofa for six hundred zlotys, and someone is behaving as though they've just invited you to operate an interbank settlement system.

And this is where a story begins that could end in three different ways. First: you recognise the scam, refuse and go back to watching your television series. Second: you begin to suspect something isn't right, but the polite buyer explains the procedure so smoothly that you eventually click. Third: a few minutes later, you're staring at your phone, wondering why, instead of receiving six hundred zlotys, you've just authorised a transaction you never intended to make.

This book exists to make the first scenario your natural reflex. Without requiring you to earn a doctorate in cybersecurity, cultivate paranoia or treat everyone interested in a second-hand coffee table as a member of an international criminal syndicate.

Online classifieds platforms are a fantastic invention. They allow us to sell things we no longer need, find second-hand equipment at a good price and pass on objects that are

doing nothing but taking up space in our homes. Thanks to them, an item can enjoy a second life while your home reclaims a little floor space. The problem is that wherever strangers, money, haste and the internet come together, people also appear who have decided to make a living from other people's trust.

Some scams are primitive. The message looks as though it was automatically translated from a language the writer has never actually heard, while the link leads to a website with an address resembling a password invented by a cat walking across a keyboard. Others are considerably more convincing. A scammer may know the name of a popular platform, use its graphics, imitate messages from a courier company or pretend to be a bank employee. They can sound calm, polite and authoritative. Sometimes they seem more familiar with the procedures than the company's actual customer service department.

The most important thing, however, is that a scammer doesn't need to be a brilliant computer expert. They simply need to understand people.

They know that sellers are delighted when they find a buyer quickly. They know that buyers worry about missing out on an attractive bargain. They know that most of us want to complete a transaction efficiently, avoid looking suspicious and refrain from asking questions that might sound stupid. That's why a scammer rarely opens a conversation with, "Good morning, I'd like to steal your money." Instead, they offer a convenient solution, reassure you that everything is safe and suggest one small additional step.

That small step can turn out to be the most expensive click in the entire story.

Interestingly, you don't have to be someone who struggles with technology to become a victim. You might use online banking every day, shop on your phone and understand perfectly well how card payments work. Yet you can still be caught off guard when your attention is focused on something entirely different. After all, you don't sit down at your computer intending to take part in a cybercrime detection exercise. You want to sell a child's bicycle, buy a second-hand phone or finally get rid of a cabinet that has been blocking access to an electrical socket for the past two years.

Scams exploit precisely that ordinary, everyday situation.

There's also the other side of the transaction. Buyers have reasons to be cautious too. An attractive price, excellent photographs and the assurance "perfect condition, used only a few times" don't automatically mean that the item actually exists. There are fake listings, attempts to obtain advance payments under false pretences, pressure to pay outside the official system and parcels whose contents bear about as much resemblance to the description as a photograph of a luxury hotel does to spending the night in a broom cupboard. Not every unsuccessful transaction is a scam, however. Sometimes the seller genuinely failed to notice a defect, the courier mixed up the parcels or the two parties understood their agreement differently. Learning to distinguish a mistake, a dispute and deliberate fraud is just as important as recognising suspicious links.

I'm not going to try to convince you that the internet is a jungle where a criminal with a laptop and a sinister laugh lurks behind every listing. Most everyday transactions can be carried out normally and safely. The aim is something far more practical: to learn to recognise the moment when

ordinary buying or selling begins to resemble a performance directed by someone who wants to take control of your decisions.

In this book, we'll examine why it's so easy to trust a seemingly credible message, how fake payment confirmations work, what a request for a code, card details or additional authorisation might mean, and why an urgent message supposedly sent by a courier doesn't always come from a courier. We'll also look at choosing offers safely, checking sellers, agreeing on transaction terms and documenting arrangements so that, if trouble arises, you're not left with nothing but a message thread entitled "But You Promised."

We won't build our sense of security around a single magic rule. The popular warning "never click on links" sounds impressive, but it teaches very little on its own. A link might lead to a genuine website or an expertly prepared imitation. Similarly, not every request for additional information indicates a crime. Context matters: who is asking, why they're asking, which channel they're using, whether you can verify the request independently and what you're actually authorising. Staying safe isn't about memorising a hundred prohibitions. It's about understanding a handful of mechanisms that keep appearing in different disguises.

Another important question is what to do when something has already gone wrong. Because someone who realises they've made a mistake after clicking needs concrete actions, not a lecture about how they should have been more careful. Depending on the situation, it may be necessary to contact the bank quickly, block a card, secure an account, preserve evidence or report the matter to the

appropriate authorities. Not every loss can be reversed, but delaying action and feeling ashamed can make matters worse. Nobody has ever recovered their money simply by spending three hours calling themselves an idiot.

And if nothing like this has ever happened to you? All the better. The cheapest lesson about scams is the one you don't have to pay for with your own savings.

You don't need to stop trusting people after reading this book. You simply need to stop treating politeness, urgency and professional-looking messages as proof of credibility. You can continue selling, buying, negotiating and enjoying a good bargain. The difference is that before following an unusual instruction, you'll ask yourself a few useful questions and independently check whatever can be checked, rather than relying solely on the person you're dealing with.

Because when you're selling a sofa, the buyer should be interested primarily in the sofa.

And if they're more interested in your card number, it's worth considering that perhaps they aren't actually looking for somewhere to sit.

Chapter 1 - When an Ordinary Listing Turns Into a Trap

You're putting a coffee machine up for sale. It works, looks respectable, and its only real flaw is that lately it has spent more time decorating the kitchen counter than making drinks. You set the price at three hundred zlotys, add some photos and publish the listing. Less than five minutes later, someone gets in touch. They don't ask about the brand, the machine's condition or why you're selling it. They don't even try to knock twenty zlotys off the price, which, in the world of online classifieds, is almost as unusual as spotting a unicorn in a supermarket car park.

The buyer says everything is perfect. They want to pay immediately and arrange a courier. They send you a link to confirm the transaction. It looks professional, features familiar graphics and displays a message saying that the money is waiting to be collected. All you need to do is enter your payment card details.

For a moment, you wonder why your card is needed when you're supposed to be receiving money. But the buyer replies quickly, politely and confidently. They explain that this is how the new payment system works. They add that they've used it many times before. Finally, they remind you that the courier will be arriving shortly, so it's best to get everything sorted out immediately.

You've just entered a situation in which the entire transaction is no longer really about the coffee machine. The most valuable product has become your attention.

Why is it so easy to mistake interest for credibility?

When we sell something online, we expect a particular sequence of events. Someone notices the listing, asks a few questions, we agree on the terms, payment takes place and the item changes hands. If the buyer is polite and declares that they're ready to pay, we automatically fit them into that familiar scenario. Our brains don't analyse every message as a separate piece of evidence in a criminal investigation. They rely on previous experiences, recognise familiar patterns and try to conserve energy. If we treated every everyday conversation like the interrogation of a suspect, ordinary shopping would take longer than renovating a flat.

Scammers exploit this natural tendency to simplify reality. Their messages often begin exactly as genuine conversations should. They ask whether an item is available, confirm their interest, and suggest payment and delivery arrangements. Only later does something appear that changes the nature of the transaction: an unusual link, a demand for personal information, an additional fee or the need to authorise an operation.

It's worth understanding that online fraud rarely consists of one enormous lie. Much more often, it's a sequence of small steps, each of which appears to follow reasonably from the previous one. First, you agree to the sale. Then you agree to shipping. Next, you agree to check some information. Finally, you may be asked to do something you would never have accepted if it had been suggested at the very beginning of the conversation.

It's rather like someone coming to inspect your refrigerator and, ten minutes later, convincing you that buying it requires access to your bank account. If they'd opened with that suggestion, you would probably have shut

the door. But when a story is presented in just the right way, even the absurd can begin to look like an official procedure.

Three sides of the same transaction

An ordinary classified advertisement involves at least two people: the seller and the buyer. Often, a classifieds platform, payment service provider or delivery company is involved as well. Each participant has a particular role. The seller offers an item, the buyer pays for it, and the other parties may help process the payment, facilitate communication or arrange delivery.

The problem begins when one person tries to take over the roles of everyone else.

Imagine a buyer who personally sends you a link to a supposed payment system, explains how that system works, assures you that it's safe and informs you that everything has been approved. All your information about the transaction comes from a single source. You have no independent confirmation, yet you may still get the impression that you're participating in a process overseen by several professional organisations.

This is one of the most important traps: confusing information provided by the person you're dealing with for information verified by an independent system.

If someone writes that they've paid, that doesn't necessarily mean the money has actually been transferred. If they send you a screenshot of a bank transfer confirmation, you have no guarantee that the document is authentic or that the transaction was completed successfully. If you receive a message resembling a notification from the platform, you should check it through the official website or application, which you open yourself.

A screenshot is a picture. It can represent reality, but it can also represent a reality that never existed. Likewise, a photograph of someone standing next to a luxury car doesn't prove that they own it. Perhaps they simply asked the real owner to move away from the bonnet for a moment.

Warning signs don't always look like warning signs

Many people expect a suspicious message to look suspicious. Language mistakes, strange characters, foreign telephone numbers or unnatural expressions can indeed be warning signs. But you shouldn't become too attached to the image of a clumsy scammer whose messages are so badly written that even autocorrect refuses to cooperate.

Modern scam messages can be grammatically correct, polite and tailored to the item you're selling. A scammer may answer your questions, mention the city where you live and even refer to specific details from your listing. None of this proves honesty. It simply means someone has read your advertisement or used information you've made available yourself.

That's why examining the purpose of someone's requests is more useful than judging their writing style. Does the request genuinely follow from the transaction you've agreed on? Is the action really necessary? Can you complete it through the official service rather than using a link someone has sent you? Do you understand exactly what will happen when you confirm it?

When selling an item, a request for your full card details, CVV/CVC security code, authorisation codes or online banking login information simply to receive payment is particularly concerning. An ordinary bank transfer into your account doesn't require you to disclose this information to

the buyer. Official payment systems may have their own procedures, but you should learn about those procedures through a trusted application or website, not through instructions supplied by a stranger.

This doesn't mean that every unusual request automatically proves criminal intent. Sometimes a person genuinely doesn't understand the platform's rules, uses a different delivery method or simply explains their intentions awkwardly. The important difference is how they respond when you try to verify the information calmly. An honest buyer might become impatient, but they shouldn't demand that you disclose confidential information or approve an operation you don't understand.

Trust isn't an unlimited subscription

People often approach transactions in black-and-white terms. They either trust someone or consider them suspicious. In reality, trust can be granted gradually and only to the extent genuinely required.

You can trust someone enough to answer a question about an item's condition. You can agree on a collection time and payment method. But that doesn't mean you have to share information about your card, your account history or codes received from your bank. The fact that someone has completed one legitimate step doesn't entitle them to demand whatever they like next.

Suppose you're selling a second-hand camera. The buyer asks for an additional photograph showing the model number and lens. That's a reasonable request, although when taking the picture, it's worth watching out for documents and other private information visible in the background. Next, the buyer asks whether you can send the

camera by post. That also falls within the normal course of a transaction. It's only when they demand that you log into your bank through a website provided in their message that you cross a boundary completely unrelated to selling a camera.

The boundary of safety, then, doesn't lie between talking to a stranger and remaining completely silent. It lies between sharing information needed for a transaction and granting access to your money and accounts.

There's a simple principle worth remembering: agreeing to one thing doesn't mean agreeing to everything the other person might dream up later.

The first minute of common sense

The most useful skill at the beginning of a transaction is knowing when to stop because someone has suddenly changed the rules. You don't need specialist knowledge to notice that you were planning to sell an item and the conversation has unexpectedly turned towards your banking information.

You can use a quick check consisting of four questions:

1. What exactly am I selling or buying, and what terms have we already agreed on?
2. What new action is the other person asking me to take, and why?
3. Can I independently confirm that this action is necessary through an official source?
4. What am I risking if I do it without checking?

These questions are particularly useful when the other person is trying to rush your decision. Answering them doesn't require a lengthy investigation. You simply need to

pause the conversation, open the official application and check whether the transaction or required action actually exists.

If a message claims there's a payment waiting to be collected, but you can't find a corresponding event in the official system, don't try to fix the situation by following additional instructions from the buyer. First, establish whether the notification is genuine.

The buyer may well protest. They might say they don't have time, that they've already paid and that you're making a simple transaction unnecessarily complicated. In that situation, a calm response is enough: "I'll complete the transaction only through the official system. I don't open external links to confirm payments."

You don't need to justify that decision across fifteen messages. Selling safely isn't a competition to see who can produce the most convincing argument.

When there's a genuine person on the other side

There's an important qualification here. Excessive suspicion can make perfectly normal transactions difficult. Not every buyer who replies quickly is a scammer. Not everyone who accepts the asking price without negotiating is preparing a fraud. Some people genuinely need a second-hand chest of drawers, know how much they're prepared to pay and have no desire to conduct negotiations resembling a parliamentary debate.

The goal isn't to create a list of personality traits that will help you identify criminals. Such a list would be unreliable. What's more important is observing specific behaviours involving money, information and control over the transaction.

Collecting an item in person is a good example. A buyer may ask to inspect the item and suggest paying when they collect it. There's nothing unusual about that. The seller, in turn, can agree on a meeting place, request punctuality and clearly establish the conditions. Caution in this situation means choosing a sensible location, protecting your privacy and making sure payment has actually been received before handing over the item.

If someone pays in cash, you can calmly check the amount you've received. If they pay by bank transfer, you should verify that the money has actually reached your account rather than relying solely on a message or an image of a payment confirmation. When an official payment or buyer-protection system is used, you need to follow its current rules and check the status through your own account.

These actions don't mean you're accusing the other person of dishonesty. They're ordinary elements of a responsible exchange.

In a restaurant, you don't insult the waiter by checking your bill. Similarly, a buyer shouldn't feel offended simply because you're verifying payment. Although, of course, you can perform that check with an expression suggesting you've just uncovered an international conspiracy involving the sale of a second-hand bedside lamp. In that case, the atmosphere may become a little tense.

The most important difference

In an honest transaction, both parties are working towards an exchange: an item in return for the agreed payment. There may be questions, negotiations and practical

complications along the way, but the fundamental purpose remains clear.

In a scam, the item often becomes nothing more than an excuse to make you perform another action. The scammer may have no interest in buying or selling anything at all. They need your data, your money, access to your account or authorisation for a transaction. That's why it's worth paying attention not only to what the other person says, but also to the action they're consistently trying to lead you towards.

If a conversation about a second-hand coffee machine becomes less and less about the coffee machine and more and more about your bank, something has clearly changed direction.

The next time you receive a message from an exceptionally determined buyer, you don't need to assume the worst automatically. You can reply, agree on the details and calmly continue with the sale. But preserve your right to independently verify every action involving your money or confidential information.

A good buyer wants to complete the transaction. A scammer wants you to stop asking questions.

And that's precisely why a few sensible questions can be worth more than the most advanced spam filter.

Chapter 2 - Why Does a Scammer Sound More Convincing Than Your Own Common Sense?

It's 9:43 p.m. You're sitting on the sofa, scrolling through messages and wondering whether it's worth making another cup of tea when you should really be going to bed soon. Suddenly, your phone announces a new notification. Someone wants to buy your second-hand mobile phone. The asking price is eight hundred zlotys, and the interested buyer declares that they're ready to pay immediately.

Normally, you'd read the message, reply and return to whatever you were doing. This time, however, the conversation quickly gathers pace. The buyer explains that they need fast shipping because the phone is intended as a gift. They assure you that payment has already been made, but the system requires additional confirmation. A moment later, they send a screenshot, followed by a reminder that the transaction could be cancelled unless you complete the procedure within a few minutes.

You're not particularly gullible. You know how to use the internet, and you have absolutely no intention of handing money to random strangers. And yet, somehow, you begin acting faster than you normally make decisions.

Why?

Because the scammer isn't trying to persuade you through arguments alone. They're trying to influence the conditions under which you make your decision.

Urgency changes the way we think

Imagine two situations. In the first, someone asks whether you'd be willing to enter your card details on an unfamiliar website to receive payment for a phone you've sold. You have time to think. You would probably consider the suggestion suspicious.

In the second situation, you're told that the buyer has already paid, the courier is waiting for confirmation and the system will terminate the transaction in five minutes. You're no longer calmly analysing whether the entire procedure makes sense. Instead, you're wondering what you need to do to avoid losing the sale.

That's an important difference. A sense of urgency can shift your attention away from the question "Is this safe?" and towards "Will I make it in time?"

Scammers understand the value of this shift extremely well. That's why they use messages suggesting that an offer is about to disappear, a payment will be reversed or the opportunity to collect money will expire. They don't always resort to direct threats. Sometimes a polite reminder is enough: "Please confirm quickly, because I can't wait much longer."

Real transactions can involve time constraints too. A buyer may have only one free evening, while a seller may need a quick decision. Urgency alone is not evidence of fraud. It becomes particularly dangerous when someone uses it to pressure you into an action you don't understand or cannot independently verify.

The simplest response is this: don't allow someone else's deadline to replace your own assessment of safety.

If a transaction requires you to perform an unfamiliar action involving money, stop. Even if the other person insists

there are only three minutes left. Losing an opportunity to sell a second-hand phone is less painful than losing money from your bank account.

What's more, a legitimate transaction that cannot survive the few minutes needed for verification probably deserves some additional thought anyway.

Authority that nobody has verified

Another way to gain someone's trust is to invoke the authority of institutions. The scammer is no longer speaking merely on their own behalf. They claim to represent the classifieds platform, payment department, courier company or bank. They use names, logos and terminology designed to create the impression of an official procedure.

People generally take institutional communications more seriously than random messages. That's understandable. Banks really can send important information, platforms may require certain actions, and couriers sometimes need additional details to deliver a parcel.

The problem is that merely claiming to represent an institution doesn't establish the sender's identity.

A message signed "Security Department" doesn't automatically become secure. A company's logo can be copied. The sender's displayed name can be misleading, as can the telephone number appearing on your screen. Even accurate knowledge of your name and details from your listing doesn't prove that you're speaking to an authorised employee.

A scammer might write: "In accordance with the payment operator's procedures, identity confirmation is required." It sounds serious. Especially when accompanied by

information about transaction security, a reference number and assurances that every step is entirely standard.

But professional terminology is not proof of professional origins. You can describe an absurd action in extremely elegant language. The sentence "To finalise the transfer of funds, please authorise a debit from your account" may still mean that someone wants to take money from you. Dressing a dishonest request in a smart suit doesn't change what it is.

That's why you should verify the authenticity of a message outside the channel indicated by the suspicious person. If someone claims to represent a platform, open its official application yourself. If they claim to be a bank employee, end the conversation and contact the bank through a telephone number or application you know from a reliable source.

Don't use the telephone number supplied by the very person whose identity you're trying to verify. That would be rather like asking a stranger whether they're a scammer and then accepting their answer, "Of course not," as sufficient proof.

Politeness that comes at a price

Not every manipulation relies on fear. Some exploit our good manners.

A buyer may be exceptionally pleasant. They write in complete sentences, apologise for contacting you late, thank you for your replies and patiently explain what they need. They mention that they're looking for a gift for someone close to them, that they've recently moved to another city or that collecting the item quickly is particularly important.