THE PSYCHOLOGY OF SCAMMING

Trust and safety in the online marketplace

Gumtree

UCLC Consulting with experts

WMG THE UNIVERSITY OF WARWICK

Trust and safety in the online marketplace

The psychology of scamming

Contents

04 Foreword

06 Executive summary

10 The scamming landscape

12 The impact of UK scamming on trust and safety

14 Spotting a scam

20 The stories of real-life scam victims

22 Why were they scammed?

23 What did scam victims learn from their experience?

24 What does a former real-life fraudster think?

26 Views from the industry

28 How the industry needs to move forward

32 Acknowledgements

Foreword

By Morten Heuing
General Manager, Gumtree UK

Nature of the beast

There are plenty of scare stories when it comes to fraud. But scamming is nothing new – since the first humans started bartering for goods and services, there's always been a minority of individuals with a poor moral compass.

Millions of people safely transact on websites every day. But there are always going to be groups looking to exploit wherever there is an exchange of money, such as is facilitated via classified platforms. There are criminals out there who have an intuition into how people behave, allowing them to part innocent victims from their cash.

In this report, we want to examine the behaviour of both scammers and victims, digging into the reasons why fraud can be an issue for online marketplaces. We want to illustrate the scale of the problem and understand the psychology behind scamming, providing advice to help consumers (whether buyers or sellers) overcome some of the challenges faced and make full use of the opportunities online marketplaces (such as Airbnb, eBay, Gumtree or Facebook Marketplace) can bring.

Why this is important to Gumtree

Used by more than one in three adults every month, Gumtree is the UK's number one classifieds site. With more than 2 million adverts[1] live at any one time, we're likely to have something for everyone, whether that be a new sofa, smartphone, job, car or flat.

As well as putting in place technology to make it as hard as possible for fraudsters to operate, Gumtree aims to make people feel safe. We would like to find ways to increase trust and safety in online marketplaces, of all shapes and sizes.

Why this is important to the industry

A lot of insightful research has been carried out in the cybercrime space. For example, the police came up with a National Policing 'Cybercrime' Protect strategy, and worked with Action Fraud to produce the 'Little Black Book on Cyber Crime'. There is also the annual release of the Crime Survey for England and Wales. And in the academic space, there was the Detecting and Preventing Mass-Marketing Fraud project, developed by the University of Warwick.

But what we also need is an open and honest conversation about who's being affected by scams. It's not 'somebody else's problem'. From our work, we know that anybody, young or old, can be a victim. It doesn't just happen to 'other people'.

The industry needs to make it clear that simply focusing on technology isn't enough – it's also a mindset change we need. As businesses, we all have a responsibility to provide as much help and advice to the public as possible in avoiding all types of scams.

This report represents a ground-breaking moment for our industry in recognising the reality of scamming in the UK. We're stronger working together, bringing together organisations to align and tackle this important issue.

[1] Source: Gumtree, June 2017

Executive summary

The psychology of scamming research highlights the problems of scam victims in the online marketplace, and the tactics criminals are using to target users.

Alongside the research findings, we worked with academic cybersecurity experts Professor Monica Whitty of the University of Warwick and Professor Angela Sasse of University College London (UCL). They helped us analyse the findings, providing valuable insight on the scam victims we interviewed.

> For the last 10 years, I have researched and published widely on 'The psychology of scamming'. I continue to lead inter-disciplinary teams and work with governments, the third sector and industry across the world to understand the problem. Through the science, I develop and scientifically evaluate novel methods to detect and prevent scams.

Professor Monica Whitty, Cyber Security Centre, WMG, University of Warwick

> I've been researching how people use security mechanisms for 20 years. That research has shown that most people want to be secure – yet they do not follow the advice of security experts. In most cases, it's because the advice is confusing, or following it would take too much time and effort, when most of us have increasingly busy lives.

Professor Angela Sasse, Professor of Human-Centred Technology at UCL, and Director of the UK Research Institute in Science of Cyber Security (RISCS)

Key findings

Gumtree spoke to 2,000 consumers, consisting of nationally representative UK adults. It also supplemented the research with a robust sample of 1,000 scam victims, to build a clearer experience of their experiences using online marketplaces such as eBay, Gumtree or Facebook Marketplace.

The cost of marketplace scamming is

£1.59 billion[2]

Victims are often scammed multiple times, losing on average £63.76, rising to £91.27 among those aged 65+.

Consumers continue with suspicious transactions

More than half (55%) of scam victims suspected they were being scammed early in the transaction process. Of those that recognised they were being scammed, more than a third (35%) continued as it was a low-value transaction, with three in ten (29%) seeing it as a bargain worth the risk.

Consumers are

not protecting themselves

Users of online marketplaces aren't taking sufficient precautions, with fewer than half (46%) checking properly before finalising the transaction to see if an item is real. Only a quarter (25%) look at safety advice, with nearly two fifths (29%) rarely or never looking at safety advice at all.

Online marketplace scams are hard to spot

Most Brits (93%) are not able to correctly identify all the fraudulent adverts we showed them – only fewer than one in 10 (7%) could guess that eight online marketplace adverts presented to them were fake.

The true cost of online marketplace scamming is

alarming

More than a quarter of Brits (27%) have been victims of an online marketplace scam, while nearly two fifths (39%) have been victims of an attempted scam.

Many online marketplace scam victims are

too embarrassed

to report incidents

Almost a fifth of scam victims (15%) didn't report, and of those that discussed the scam, four out of 10 (39%) said they felt stupid for having fallen victim, with more than a quarter (28%) thinking it was their own fault.

This is 51,339,000 adults
27% = 13,623,693
*1.8 incidents = 24.918.434 incidents
*£63.76 = £1,588,697,899

The scamming landscape

Popular online marketplaces and applications (such as eBay or Gumtree) exist where product and service information is provided by multiple users, with the aim of conducting successful transactions. Gumtree is an online classified marketplace run by operators that don't own any inventory, who facilitate the initial contact between buyer and seller.

These websites and applications are very popular, because they allow consumers to take part in a socio-economic system called the 'sharing economy', in which internet users can share assets, as well as products and services, with one another. This benefits them because they can save money and find items which they might not be able to using traditional shops or ecommerce sites. It also allows everybody to make use of underused resources, from electronic goods and cars to room space they can rent out.

Online marketplaces are like beehives, in which users are following principles and set rules of exchange. It relies on people for its success, and that's why they are such exciting and entrepreneurial places to inhabit.

Why are criminals attracted to online marketplaces?

Online marketplaces that give people the freedom to buy and sell goods to one another will always attract scammers – unruly users looking to exploit weaknesses in the human psyche, just like offline criminals have done for centuries. Right now, the science to detect scammers is still rudimentary – which means many of them slip through the net.

What Gumtree does to tackle fraud

Gumtree is focused on making the user experience as safe and secure as possible. Adverts caught by automated filters or reported by users are rapidly blocked, if they are believed to be fraudulent. We also regularly invest in new technology which is designed to combat the evolving techniques used by scammers.

For example, Gumtree automates the detection and removal of sites pretending to be part of the platform, using keywords to filter and block offending adverts. The organisation also uses data to identify fraudster patterns, links and trends, with the automatic blacklisting of IP addresses taking part in suspicious activity. Gumtree continually analyses and updates systems to catch criminal activity.

Gumtree partners with organisations such as the police to identify fraudsters, and the business has built valuable relationships with groups such as Get Safe Online and Action Fraud to share learnings and best practice.

On the Gumtree website, there are dedicated sections which guide users to make a safe exchange, whether they're looking to sell a car, find a place to live, or find a new job. Users are encouraged to report suspicious behaviour with a 'report it' button.

What scamming guidance exists?

There's a lot of guidance already available through different sources, whether it's advice given by online marketplaces themselves, or tips given by the police or an industry body. However, research and conversations with stakeholders shows that this advice is inconsistent, often causing confusion and a false sense of security.

Gumtree is seeing that many consumers aren't savvy on matters of trust and safety. They find advice hard to find and it doesn't come at key moments on their online journey. Some of it is simply poor – stating the obvious or urging people to be more 'vigilant'. Even if not vague or hard to action, safety guidance can fall short if not presented in a consumer-friendly way, and scare people off.

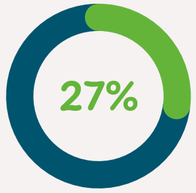
> Currently, consumer guidance from government comes in many forms. The longest-established one is Get Safe Online, which is a resource of advice on keeping specific devices and operating systems, for example secure. It also warns of current scams. The advice tends to be the same – don't click on links, don't open attachments, put the phone down, report to Action Fraud.
>
> Cyber Aware (formerly Cyber Streetwise) focuses on promoting protective behaviours – protect your device (via software updates), protect your data (with strong passwords), and protect your business (via Cyber Security Essentials). Rather than warn of specific scams, Cyber Aware works with 300 partner organisations to help them create their own awareness communications.
>
> Since its inception in 2016, the National Cyber Security Centre (NCSC) has been providing both general and topical advice to UK organisations. Its advice is mostly aimed at larger organisations who employ IT and security specialists, giving authoritative, up-to-date technical advice on how to protect systems.
>
> Recent topical advice (for example, after the ransomware attacks) also offered specific advice for home users and small organisations (having backups and updating software).
>
> The different sources do not agree – while Get Safe Online and Cyber Aware emphasise the importance of strong passwords, the NCSC advice is that reusing passwords across multiple sites is the biggest risk, and recommends two-factor authentication and password managers to enable users to cope.
>
> **Professor Angela Sasse, UCL**

The impact of UK scamming on trust and safety

Thanks to the research, we now have a good picture of scamming in the online marketplace today.

The cost of online scamming is

£1.59 billion



have been victim of an online scam

have been victim of an attempted scam

More than a quarter of Britons have fallen victim to an online marketplace scam

More than a quarter of Britons (27%) have been victim of an online marketplace scam, while two fifths (39%) said they had been the target of an attempted scam. On average, individuals have been scammed between one and two times in their lifetime, and target of an attempted online marketplace scam three to four times.

The estimated cost of online marketplace scamming is in the £1.59 billion region. On average, a scam victim loses £63.76 in each incident – scammers using online marketplaces picked their targets carefully, usually picking low-value transactions, such as for sale items.

Britons are most vulnerable to a scam with for sale items. The most popular categories that scammers target in the online marketplaces we looked at were:

For sale items	43%
Automotive	14%
Jobs	8%
Services	7%
Community	5%
Property	5%
Pets	3%

Only 7% of Britons could identify all the scams that were shown to them

Brits aren't good at detecting online marketplace scams

As part of an exercise, researchers showed eight adverts to respondents and asked them to identify which ones were scams. Only 7% could identify all the scams that were shown to them. Those who had been victim of a scam were more likely to detect all the fake advertisements (11%). Red flags were based on price, detail, look, gut feel and wording.

The percentage of correctly identified scams:

Smartphone (fake)	66%
Construction toy (fake)	54%
Flat (fake)	47%
Motorhome (fake)	41%
Steering wheel (fake)	39%
Car (real)	32%
Trendy cooker (real)	31%
Rug (real)	26%

Spotting a scam

This is a selection of comments made by Britons on the reasons they found a fake advert suspicious.

"Not a lot of detail, too much small **detail**"

"The language is not good, ambiguous **wording**"

Detail

- "No Oxford Tube in Westminster"
- "Private ad but states they accept credit card payment"
- "Not a lot of detail / too much small detail"

Wording

- "Adverts were poorly spelt and some information was missing"
- "Sounds unbelievable"
- "The language is not good, ambiguous wording"

Look

- "It doesn't look genuine"
- "Pictures look dodgy"
- "They look photoshopped"

Price

- "£550 is a crazy price"
- "£45 seems too cheap"
- "Think it would be worth more"

Gut feel

- "Educated guess based on gut instinct"
- "Sounds unbelievable"
- "Something about it doesn't ring true"
- "Naturally sceptical"

Example of a fake advert

Studio flat for rent. Ground floor property. - Read the description before replying to the ad!!

Westminster, London — £550.00pm

Posted	3 hours ago	Property type	Flat
Seller type	Private	Room type	Double room
Date available	06 Nov 2016	Available to couples	No

Description

"Ground floor studio flat for rent in a quiet side street

This fantastic studio is on the ground floor, providing you very quiet and private living environment. The property is located just close to the Oxford tube, so it's very convenient for students in both UoM and MMU.

This is a beautiful studio flat with open plan kitchen and new wooden floor. Quite big for Manchester, larger than usual - 65sqm total area.

open plan kitchen / living area - double bed and storage - L shape sofa - glass table with chairs,armchairs - shower room - secure complex - bike storage

The price contains all the bill, including even TV licence and very fast internet access. You can enjoy gym, studying room, weekly room cleaning service, party and also film and sports event for free! I'm sure you will be very satisfied with this stylish studio apartment.

Would suit ideally for a professional couple or a single person or student. Off-street parking lot is included in rent.

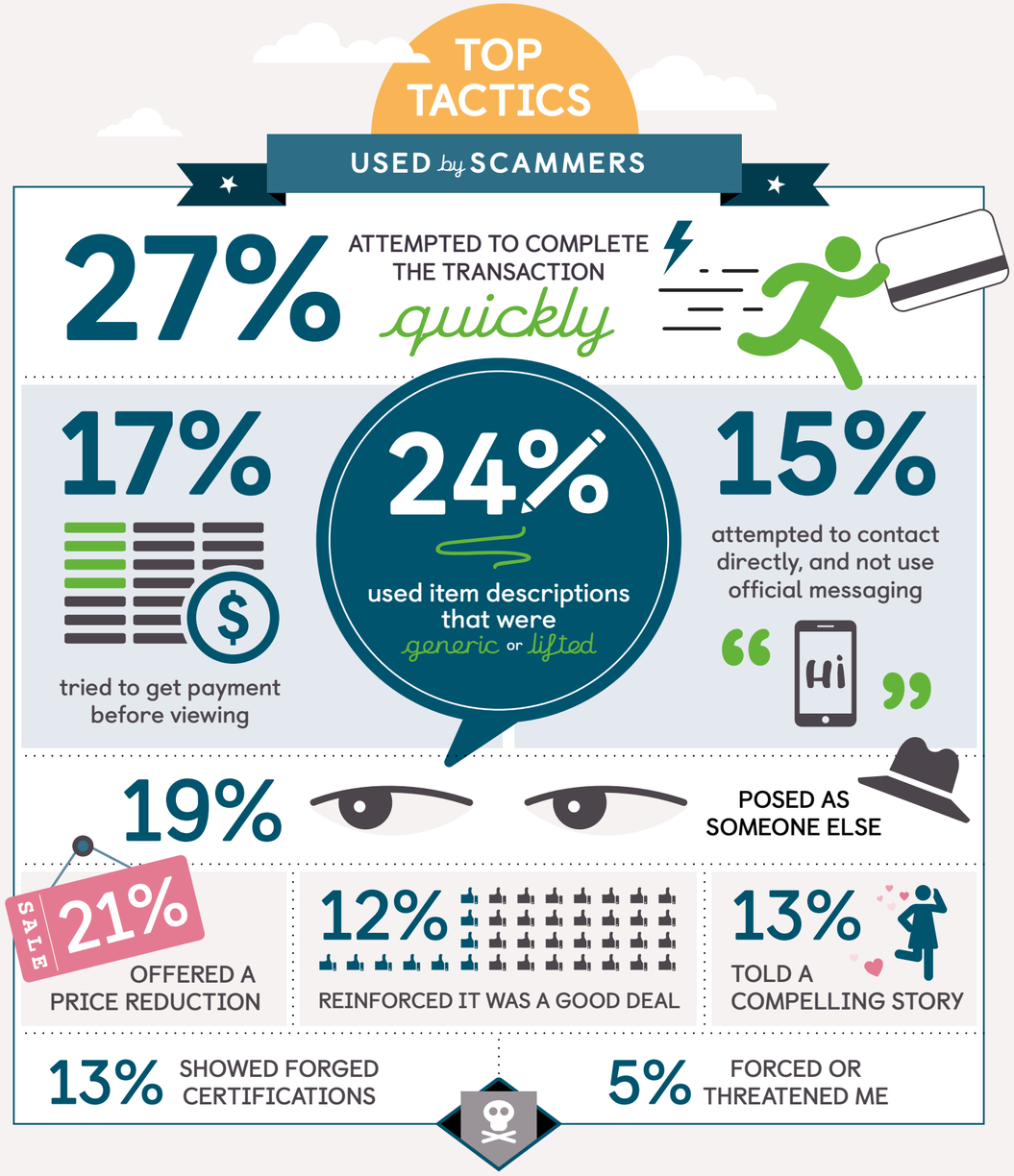
Loads of lovely and cool pubs, cafes, restaurants are just a stone throw away.

Ad ID: _____

"£550 is a crazy **price**"

"They **look** photoshopped"

"Educated guess based on **gut instinct**"



Falling victim to an online marketplace scam

We asked scam victims what kind of tactics were used against them. The most common included attempts to speed up a transaction (27%), using generic images and descriptions (24%), or attempting payment without a buyer seeing the item (17%).

We also asked scam victims what they thought their own weak spots were. There were numerous reasons, which included their need for a bargain (17%), convincing adverts (17%), and the belief that it couldn't happen to them (21%).

The reasons scam victims went ahead with a transaction:

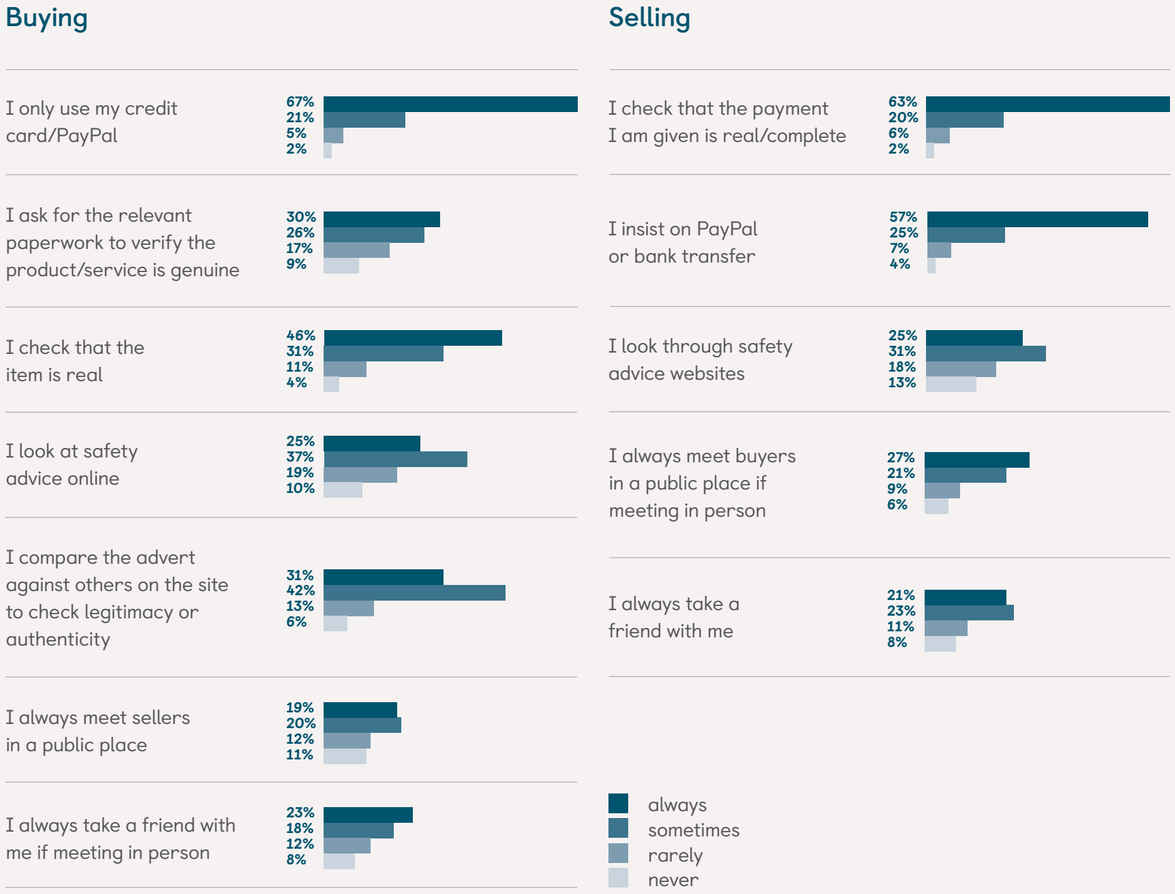
I trusted the seller	21%
I thought it could never happen to me	21%
I wanted the product or service	19%
I thought it was a bargain	17%
I thought the advert was convincing	17%

> "I have investigated the tricks criminals use and the reasons why individuals are conned into parting with their money. I focused on cyber-enabled scams, revealing elements of the online environment which makes a scam more convincing. The psychological impact of some types of scams can be quite traumatic – leaving the victim ashamed and blaming themselves – rather than the criminal."
>
> **Professor Monica Whitty, University of Warwick**

Most Britons don't look at safety advice offered by online marketplaces

Britons often rely on payment safeguards, rather than their own knowledge of online marketplace trust and safety. The most widely used precaution when buying and selling through online marketplaces is the use of a credit card or PayPal, with only a quarter of Britons (25%) looking at safety advice when it came to buying and selling in the online marketplace.

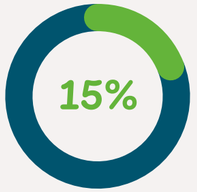
What precautions do you take when buying in an online marketplace?



Even with suspicions, many online marketplace scam victims moved forward with a transaction

One surprising finding from the research was the fact that victims admitted to moving ahead with a transaction, even after suspecting they were in the process of being scammed. Generally, it was because they thought there was a minimal risk with items of low value.

The analysis found that nearly a fifth (15%) of scam victims didn't report the incident, because they felt nothing would come out of it, or that it was their fault.



didn't report the scam

At what point did victims begin to suspect they were being scammed?

During the initial conversation	35%
After speaking to them for a long time	25%
When they asked for money	22%
As soon as they saw the advert online	20%
After money had been taken	19%
Never suspected	9%

The top signs that made victims realise they were being scammed

Offer too good to be true	36%
Details requested that were not usually asked for	29%
Poor spelling and grammar in advert or correspondence	28%
Text/images for the advert were generic and found elsewhere on the Internet	17%
Asked to pay for the item before it had been seen	15%
Referred to transaction that hadn't been made	15%

How did you share information about being scammed?

Through the website used	36%
Friend or family member	35%
Bank	30%
The police	17%
Review forums and social media	16%
Review forums and social media	15%

The stories of real-life scam victims

As part of the research, online marketplace users were asked about their experiences of falling victim to a scam.

The smartphone scam

"I saw a smartphone which looked reasonably priced and in good condition, to buy for my son. I contacted the buyer and he was relatively quick to reply. With my son, I agreed to meet him face-to-face.

The seller advised that the phone was running out of battery – but he assured me it was working fine while en-route. By the time we met, there was no charge. However, the seller said it was 100% working and gave me a landline number and email address in case of any problem.

I got home, put it on charge and immediately knew there was a problem. It wouldn't charge. It was completely dead, and when I got it checked out at a repair shop, they said it wasn't cost-effective to repair.

It could have been prevented if I had made more checks. I've learned from this – if I'm buying anything of any value, I'll ensure I thoroughly check it out to see if it's working. If I'm not happy, I'll walk away.

I was disappointed that somebody could blatantly lie to me, even when I had my son with me and explained it was a present for him."

Female, 45-54

The car repair scam

"Last year I sold a pickup truck for my dad on an online marketplace, with the buyer travelling to collect and pay for the vehicle. The buyer inspected the car, confirmed they were happy with it, paid the asking price and set off. Several hours later the buyer claimed he hadn't reached the border and was with the AA because he said it had developed a fault.

The buyer was with another man, who claimed he was from the AA and the car had been taken to a garage. We were confused about the situation, because the car had been MOT'd and serviced. The buyer demanded we transfer money for repairs – we declined and advised the buyer to travel back and return the car if he was unhappy.

My dad was troubled, and willing to transfer the money because he would hate being in the same situation. But he asked for a repair invoice and confirmation from AA to validate the story – neither was forthcoming.

I believe the buyer was trying to scam us. It left us with a bad taste in the mouth considering this individual had come to the house and spoken with us! We considered taking further action, but ultimately decided not to as there seemed little value in doing so."

Female, 25-34

The console scam

"I wanted to buy a gaming console, and spent some time looking online for a good deal. I thought I'd found one – it wasn't suspiciously cheap as scams often are, but seemed a good deal, with a reputable-looking company. So, I made the order, paying with PayPal.

The next day I received an email from the company's fraud department, saying they'd done a random check and wanted to confirm my address. They would send me a code via post, which I would enter on their website, and the console would be sent. The code arrived, I signed for it, but the console didn't arrive.

My suspicions were raised, because PayPal looks for proof of delivery, and now they saw something I had signed for. Attempts to reach the company failed, and I saw others complaining online about the company – it looked like they had conned hundreds of people."

Male, 45-54

Why were they scammed?

The common thread between all the scam victims that were interviewed was that the scam artists targeting them tried to play on their emotions or lull them into a false sense of security. Scams are becoming harder to recognise.

The main reasons they fell victim were:

1 A perceived good deal.

Items subject to scams tend to be slightly cheaper than others, but not so cheap to raise suspicion. This led to them initially thinking they had found a good deal.

2 Overall high advert quality.

For scam victims, good quality and genuine-looking pictures made an advert trustworthy. They were also fooled by detailed descriptions and specs, which further emphasised trustworthiness.

3 Perceived reputable source.

Lots of items for sale and UK contact details made a site or seller reputable and trustworthy. There was also a problem with reputable payment methods like PayPal, as they gave victims the illusion 'nothing could happen'.

4 Extra effort from the seller.

Initial effort and kindness from a seller raised their trustworthiness. For example, sellers would offer to come over to the house of a victim to make the transaction.

Their negative experiences made them aware of the issue and the fact that it could happen to anybody. But it's important to note, it didn't increase their knowledge of scam prevention methods.

The users we spoke to felt they only got information and advice after they were scammed and went through the process of looking for scam prevention information. They weren't aware of any advice available for scam protection, and didn't know where to access it.

"I think the ability now for people online to create false accounts and emails that seem genuine is the real issue."

Scam Victim, Female, 18-24

"My negative experience hasn't really given me a greater knowledge, but rather an appreciation. I always felt like it was something that happened to other people.

Now I don't have a greater knowledge, but I do have a heightened awareness of similar stories and appreciation for what it feels like."

Scam Victim, Female, 25-34

Scam victims believe it was their fault

One particularly worrying trend among the people we interviewed, was the tendency of scam victims to believe it was their fault. For example, they asked questions of themselves, believing themselves gullible and that they should have known better.

What did scam victims learn from their experience?

1 They need to see physical proof.

The scam victims we interviewed said they now need to physically see and test items before purchase.

2 They'll only use sites that they've had previous positive experiences with.

Before a bad experience, users are open to untested pages and sellers. Once they've had a bad experience, they'll avoid these.

3 They'll look for payment methods with guarantees.

Scam victims will look for guarantees or a two-step payment process.

4 They'll rely on reviews and ratings more.

Even if they're looking on a reputable website, scam victims will now pay more attention to consumer reviews and seller ratings.

What does a former real-life fraudster think?

Tony Sales has been dubbed “Britain’s Greatest Fraudster” by the media, allegedly stealing £30 million in six years, having committed his first credit card scam at just 13 years old. Tony was once one of the country’s most wanted men.

However, he turned over a new leaf and put his knowledge towards helping people as a fraud prevention expert. Tony reflects on the scamming victim stories, and offers his analysis on the research findings.

What did you think of the phone scam?

The woman who was scammed for the phone is a classic example of the sort of person a fraudster loves to target. She took her son with her to buy the phone – that was a mistake, as the kid was obviously going to be excited about getting it. She couldn’t see that the fraudster took advantage of her decent, hardworking honesty to manipulate her.

All the scammers use a lot of reassurance. In the phone scam, the scammer rings her and tells her that the battery is dying on the phone he’s selling, but that everything is fine with the phone. He also gives another bit of reassurance when he gives her a landline number and email. But what does that mean? Did she speak to him on any of those? It was obviously fake.

Your thoughts on the console scam?

The console scam was impressive. As a criminal, that was beautiful. You look at it and go wow – they thought the whole thing out. Even getting the signature at the end, so now he can’t complain!

The person who set up the scam has either been a victim, or is somebody who’s part of it. How would they know about the internal processes and that PayPal won’t pay out if somebody’s signed for a delivery?

There’s no real constraint when it comes to fake websites. You can bang one out, make it look good, and people will buy from it. I can copy any guarantee statement out there – it’s very easy to do. But people get fooled, just to get a console a tenner cheaper.

Some of the scam victims in our research continued with a transaction, even when they knew they were being scammed. Why is this?

Because of the low amount of money involved in these transactions, most of us will say it’s worth the punt. It’s just how we are. Our time is more important, and criminals know that.

In the shoes of a user, what would you do if you wanted to buy a car from an online marketplace, for example?

I would try and get as much information as I possibly can on that car. None of us, unless we’re mechanics, are car experts. But we all have a bit of common sense and ability to do some due diligence. But like the woman with the phone, people get excited, and it’s this that a fraudster takes advantage of.

What other advice would you give to buyers and sellers?

Look at all the little elements that look a bit strange about a transaction, such as the phone going off and not working. You’re well within your rights to ask someone to see it work before you buy it as it’s their responsibility to bring a phone that’s fully charged.

It’s about making people aware of those tiny social engineering steps that criminals take to make money. When you look at the whole thing, criminals tap into what scammers have done for thousands of years.

I think online marketplace scamming has got out of hand. There’s so many people being scammed that they’ve had enough. If we’re going to embrace the internet, everybody needs to wake up.

Do you have any advice for the industry?

I think a checklist could have helped people with many of these scams, tips on what to check before buying and selling. Having a pop-up notification could help – just telling the buyer or seller where they should be careful.

You’re never going to totally stop scamming. But you’ve got to try and interrupt it. A lot of this stuff is opportunist fraud, where criminals learn their craft – at this stage you can stop them from succeeding with these small crimes and getting involved in bigger crime.

I think websites could potentially show information about criminals who have been caught and punished for fraud. As well as reassuring users, it might act as a deterrent for criminals knowing that the website they’re scamming on will go after them.

Views from the industry

The results were presented to a panel of industry stakeholders – many agreed there was a general lack of knowledge about trust and safety, which was leading to ignorance about the best way to buy and sell in online marketplaces.

There was also concern that there was too much advice and information out there that was poor quality and inconsistent, and created a sense of mistaken overconfidence.

"If we are going to maintain confidence in our increasingly digitised economy, we must make sure that everyone, whether small or large retailers, manufacturers, voluntary bodies, academic institutions, digital market places, as well as our Government and critical networks, can carry out their business in a safe and secure UK digital environment."

Andy B,
National Cyber Security Centre

"There's a lack of knowledge and understanding about where you can find trust and safety advice, and how you can protect yourself. It's where a lot of people fall short.

I also believe that this information isn't always readily available. I think there should be a point in the buying process where the service asks you if you've made the necessary checks to ensure it's not a fraud and proactively gives you the signs to look out for.

This will lead to a better experience, because people will be equipped with the knowledge to recognise a potential fraud.

However, I know putting these types of safeguards in place is difficult. It's a balance between user security and the needs of the business – it's hard to get that right."

Evalambios Christophi,
Action Fraud

"Fraudsters understand your psychology and how you work better than anybody else. They make sure they know the security checks on each site, and they'll test them. That way if they manage to get a fake advert online, they're confident that nothing will trigger an alert.

There's lots of advice available about staying safe in online marketplaces, but people aren't always aware of it or follow it. If you stopped people in the street and asked them about trust and safety online, I don't think many would have an understanding."

Helen Fearon,
Vehicle Safe Trading Advisory Group

"Trust and safety is an issue relevant to anybody working in the online marketplace, and one which we are all keen to solve. There are several issues to deal with, but for me, getting people to opt-in to identification is very important, as is making sure that the roles of participants and platforms are clear.

Online marketplaces need to understand where their responsibilities start and where they believe their responsibilities finish. They also need to make this very clear to participants, sharing with users their processes for when things go wrong. It'll help us understand the overall extent of problems in online marketplaces, and help us get to resolution in individual cases more quickly."

Richard Laughton,
Sharing Economy UK

"Security is a key principle that underpins the success of an online marketplace; providing the foundation for consumers and businesses to confidently use a service with trust and assurance.

The online marketplaces that take online security seriously and protect their users from scams will be the ones that are most trusted and, in return, most used. That is why it is imperative that security is at the forefront of any online marketplace commercial strategy."

Julian David,
TechUK

"I did a search on the recent incident of ransomware, and I saw huge numbers of websites giving advice on different areas. A lot of media will put advice out there – there will never be consistency, because they all want their voice heard."

Tony Neate,
Get Safe Online

How the industry needs to move forward

This report brings together different perspectives, all with the aim of improving trust and safety in online marketplaces. We've heard from government and industry, researched users, and learned about scamming psychology from experts and even a reformed criminal. It's clear that this is a subject that needs attention, involvement and collaboration to move forward.

From research findings, many consumers aren't savvy about online marketplace trust and safety. Currently the advice is difficult to find, inconsistent across platforms and channels, or doesn't come at key points in the buying or selling journey of a marketplace user.

Sadly, more than a quarter of Britons have been scammed at least once. Consumers are having a hard time identifying fake online adverts – either falling for a real scam, or identifying classified adverts as legitimate. And even if they suspect a scam is happening, they'll continue the process – relying on safeguards or because it's 'worth the punt'.

Scammers play on the way we think, whether it's our desire for a bargain or a sense of urgency we have in our time-poor society. With one in five online marketplace scam victims not even filing a report, that's adding up to a challenge which we all need to face. It's stopping some users from having an enjoyable online experience.

"My work has revealed that some of the advice and warnings don't necessarily help protect victims or change their cyber security behaviours. Common advice, for example, such as: 'if it is too good to be true' is not always helpful, given the 'too good' element is often presented later down the track – once the user is already hooked.

It's paramount that we continue to:

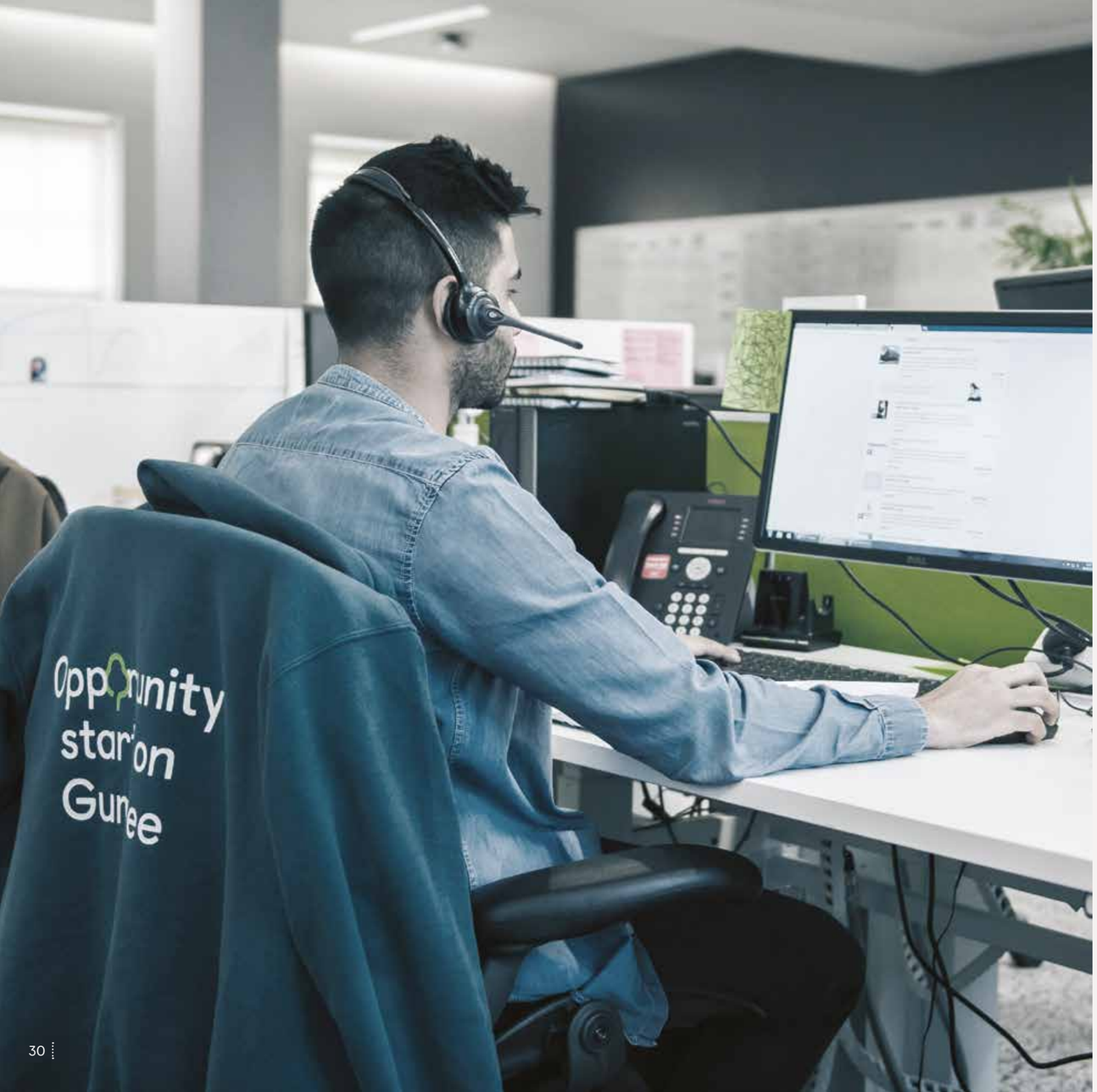
- Understand exactly how these scams operate
- Improve tools for scams to be automatically detected on websites
- Equip users with strategies to detect and question the legitimacy of the person they are communicating with online, when websites fail to detect
- Change cyber and physical security practices to make it more difficult for the criminal to defraud innocent citizens."

Professor Monica Whitty, University of Warwick

"Increasing awareness by telling people about the risks is not enough – our research has shown that most people are aware of the risks. But they are tired of confusing terminology, as well as disruptive security mechanisms like warnings and CAPTCHAs, which have no security benefits for them. They want advice that is reliable, easy to understand and simple to follow, delivered at the point when they are considering a purchase.

Most people trust service providers to try and keep them secure, e.g. by filtering out offers they can identify as scams, and blocking accounts linked with scammers. Most people are willing to contribute to that effort, e.g. by reporting scams they spot – but they want feedback that their efforts are making a difference, and how."

Professor Angela Sasse, UCL



What the future holds

What's important is what we do with the findings from this report – trust and safety is a huge issue that affects a world that is increasingly online.

Industry-wide solutions are needed, such as:

An organised bottom-up strategic approach. Such as additional industry-wide research to lock down scamming mechanisms, the examination of consumer and business needs, and the introduction of governmental regulations.

The optimising of content and delivery of consumer guidance. Based on our findings and conversation with an ex-fraudster, we must ensure that the whole industry understands the importance of context and tone of voice, landing trust and safety messages at right moments during the consumer journey.

Technological solutions to issues of trust and safety. For example, products and features adding safety to online transactions such as opt-in identification, trust scores for buyers and sellers, or pop-up messaging during the right moments in a journey.

We hope 'The psychology of scamming' moves the online marketplace trust and safety conversation forward, so we can build solid and long-lasting solutions to a growing problem.

Acknowledgements

Gumtree would also like to thank the organisations which participated in our 'The psychology of scamming' report, including:

Contact

Gumtree is committed to Trust and Safety.

If you need more information about anything in the report, please contact Fergus Campbell, Head of Public Relations at Gumtree UK on +44 (0) 7825 682372 or fcampbell@gumtree.com

Gumtree