

Navigating the Web of Deception: A Comprehensive Guide to Online Scams

by thinkbroadband.com



Foreword



thinkbroadband.com



@thinkbroadband

The internet is a force for good, helping you research issues you're interested in, compare prices of goods or services, communicate with friends and family and keep entertained, however there is a dark side and it is crucial to be mindful of the risks that come with it. We understand that staying safe online can feel like navigating a treacherous sea, but fear not! Our guide is designed to provide you with the key tips and strategies to navigate this digital landscape confidently and securely.

Ofcom's Online Fraud Report in March 2023 found that **46% of adult Internet users have personally been drawn into engaging in an online scam or fraud**, while 39% reported knowing someone who has fallen victim to an online scam or fraud.

The global nature of the Internet means it's possible for malicious individuals to exploit unsuspecting users on the other side of the world by scamming them. The worst of this is, that because it's so international, law enforcement will often not be able to help as communicating between authorities is difficult and resources are limited. The key message is you need to take control and protect yourself and your loved ones, not rely on anyone else to do this for you.

This comprehensive guide is designed to help you understand common scams, how they work, what the trademark signs of scams are so that you can avoid them, and especially share this with those more vulnerable. But be warned, you can't read about every scam out there. You must use this knowledge to build a healthy scepticism and understand the traits of scams which change from day to day.

We sincerely hope that this guide will serve as a valuable resource in your quest to protect yourself and others from the perils of online scams.

Together, let us create a safer digital environment and empower one another to embrace the boundless opportunities the internet offers.

Stay safe, stay informed, and enjoy your journey through this guide.

Sebastian Lahtinen

Director, thinkbroadband.com



Contents

3

How to spot a scam?

5

Key steps to protecting yourself online

7

A personal tale

8

Top Scams – Consumers

15

Top Scams – Businesses

19

Artificial Intelligence

How to spot a scam?

There are many different types of scams, but these are our top ten tips which should be raising your suspicions:

1. Never share your password, PIN codes or such information with callers

Unless you call your bank directly on a number you obtained from the back of your card, never share any security information with anyone. Also never share bank security information with your family or friends. If you need to give access to your account to a family member, talk to your bank and they can arrange this officially. If you share your PIN code with a family member and the bank finds out, if you then become a victim of fraud, your bank may simply tell you that you have previously shared with someone else, implying you can't be trusted not to have done so to criminals too.

2. Unsolicited contact

Scams often begin with a message or call 'out of the blue', be it by e-mail, text message, phone call, a pop-up message on your computer or something similar. You may find these are "scatter gun" approaches sent to millions of people, but only expecting a handful to fall for the scam. A message may say you need to contact the sender, so you feel like you're the one making the approach. This isn't *always* the case, but it's a common trait.



3. Do not trust the name of the sender

The "from" line on an e-mail, the telephone number that pops up on your phone when someone calls you, the text message sender – these can all be faked. Do not trust that someone who calls from your bank is actually working for your bank. If you need to verify the authenticity of a caller or message, contact the sender through your existing contact information, not any number in the message. If it's your bank, call the number on the back of your card. How easy would it be for you to write a letter to someone and on the back write someone else's address as the 'sender'? It's just that easy to send e-mails or make calls pretending to be from someone else. Never click on links in e-mails.



4. What the scammer wants

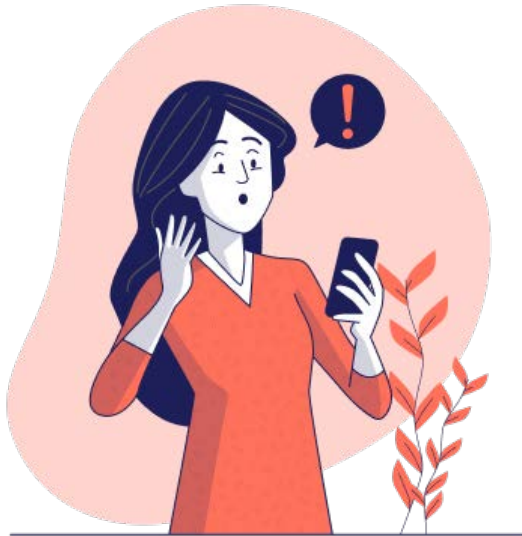
Not all scammers are wanting money, at least not first. Some may be after your personal data which may let them target you with more personalised scams later, or they may want access to your online accounts so they can use them to scam others using your reputation (many people will be more likely to help someone they know, unaware that a scammer has taken control of their account). Some scammers want money, be it payment by credit card, gift card, cash, or something else. Some scams are elaborate and long, whilst others are simple and quick.

5. Some information about you doesn't mean the sender is who they say they are

Just because the caller/sender knows your bank with a particular institution or even knows your address or credit limit, broadband provider or insurer, it doesn't mean they are actually from those companies. Any website knows which broadband provider you use (and if you guessed "BT" you'd probably find a significant number of consumers would be BT customers).

Continued ➔

How to spot a scam?



6. Secrecy, urgency and pressure (including “moral” pressure)

Most scammers will try to rush you into doing something because they don't want to give you the time to think or possibly tell a friend who might suggest it's a scam. They will tell you not to tell anyone about what they are asking you to do. They will put pressure on you to deal with the issue straight away, sometimes appealing to your honest nature to right a wrong (e.g. you received too much money for a refund and they may lose their job if you don't return it), or they may say they are from law enforcement or a government agency, making it sound official. If someone on the phone asks you to lie to anyone or say something that isn't true, your alarm bells should be ringing. If you must lie to the bank about the nature of a money transaction, not tell the cashier you're buying gift cards after someone called you, not tell your family about the issue or even tick to say you're transferring money to friends on PayPal when it's not a friend, it's almost certainly a scam.

7. Codes sent to you by SMS/e-mail

Do not share any codes (often six-digit codes) sent to you by e-mail or text message by your bank or other company with anyone you aren't sure is a legitimate person. Often these codes can be used to reset your password (e.g., with Amazon) and they prove to the company that you are legitimately making that request. If you share the code sent to you with a scammer, you're just as well handing the keys to your Amazon account to whoever called you, no matter who they are. A caller telling you they are sending you a 'security code' is a common tactic to obtain these codes, whereas in fact, all they are doing is asking the supplier to reset your password.

8. Scams are not always obvious and may be highly personalised

A decade ago, we saw the African prince who needed your help to transfer funds out of their corrupt country and an uncle who wanted to steal it. These days, scams are far harder to spot and Artificial Intelligence can make it even more difficult as each scam message will be different. Scammers can send very targeted messages or calls knowing information about you to gain your trust, and these days you won't see as many spelling mistakes or grammatical errors in messages as you used to (although if you do, that's a sign to watch out for!).

9. Not all scams are unsolicited

Some scam victims find themselves contacting the scammers without any unsolicited contact! One good example is a lot of questionable actors are buying Google AdWords which appear at the top of your search results. If you Google “applying for your first driving licence” or “how to apply for a U.S. ESTA/eVisa”, you may find a company offering to help. Often these companies offer worthless services and either charge over the odds or charge you for something that's completely free (such as an EHIC/GHIC card). These aren't “scams” but we would call them “trivial value businesses” as they often rely on you not reading the small print that explains you can get the service much cheaper or free, and you just assume this is an official website.

10. Trust your instincts

If it just doesn't ‘feel’ right, it probably isn't. A legitimate caller would never have issues with giving you their details and you reaching out through trusted channels. Don't assume that someone who sounds like they are protecting you by advising you how to contact them is acting in your interests. Make sure you only contact banks, etc. through telephone numbers you know are theirs. Don't take down details from callers or offer the option for them to call you back from a number you recognise.

Important!

We refer to a lot of legitimate companies (Microsoft, Amazon, Ebay, etc.) who scammers may pretend to work for, or scammers may use legitimate tools (TeamViewer, etc.) – These companies are not at fault, but victims of their brands or services being mis-used. We refer to them here to give you realistic examples of scams that are out there but please don't be dissuaded from using them. They are just well known enough that scammers like to pretend they work for them.



Key steps to protecting yourself online

1. Never share your password or PIN codes with anyone else, including phone repair shops

The name of your pet, the city you were born/married, London2022, etc. are NOT secure passwords. You must use different passwords for each website. If you subscribe to a forum for talking about dogs and they are hacked, and you used the same password for Ebay, your account could now be accessed by hackers to scam others using your name to commit fraud. A password manager which allows you to store passwords on the computer is helpful. (Common services include [1Password](#) for consumers and [Dashlane](#) for businesses). You can also use [iCloud Keychain](#) on Apple MacOS or password managers built into some web browsers like Chrome or Firefox.

If you haven't changed your e-mail account password for ten years, now would be a good time to do that. Finally, don't give your mobile phone PIN code to any mobile phone repair shop as they would have access to everything on your device!

2. Multi-Factor Authentication

Use multi-factor (or two-factor) authentication where possible. This means that it's more difficult for someone who gets hold of your username/e-mail/password to gain unauthorised access to your accounts or sensitive information. This will help, but be careful who you give your codes to!

3. E-mail accounts & Bank Logins

Be especially careful with the login details you use to access your e-mail account and your bank, or any other payment institution, such as Paypal. These are the most vulnerable as if someone has access to your e-mail account, they can reset a lot of your passwords. The end goal for most scammers is to get untraceable money, and these logins help with that.



4. Phone PINs password

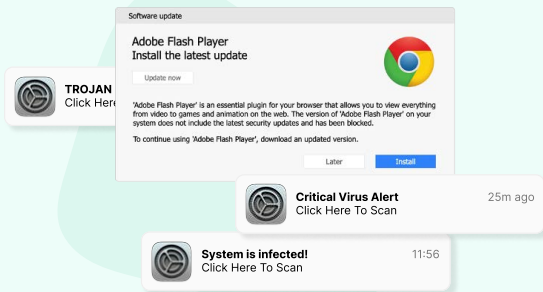
Protect your mobile phone with a PIN code of at least eight digits, and make sure your computer password is secure. If you have facial or fingerprint recognition on the phone, use that and make sure it locks immediately if you turn the display off. Your phone often has your life story and this information could be very valuable to a scammer, be it targeting you or your friends and family.

5. Remote Control Software

It is crucial to exercise extreme caution when granting access to your computer or mobile phone. Software applications like AnyDesk, TeamViewer, and UltraViewer, which are commonly used for remote support, have unfortunately become tools of choice for scammers seeking to gain unauthorised control over your devices. Whilst there are genuine reasons to use these for remote support, you should know the person on the other side to do this. There is no reason for you to download any software whatsoever for anyone who calls you, and doubly so for remote control software. Be careful sharing your screen on Zoom or Teams as well and ensure you consider the content visible on your screen. If you need IT support, go into one of the major technology stores or ask a friend/family member for help. The person on the end of the phone is not someone you should trust.

Continued ➔

Key steps to protecting yourself online



6. Pop-ups

Be cautious about pop-up notifications which warn you about out-of-date software, missing Adobe Flash Player or claiming some viruses were found. These may be generated by rogue adverts or websites. Take a photo of them, turn your computer off and ask a trusted friend for help if you're unsure.

7. Personal Data

Avoid sharing your personal details if there isn't a good reason. Don't share your e-mail address with a store because they ask to send you a receipt. Maybe consider setting up a separate e-mail address for these kinds of uses and keep other content on another address. Does a website really need your date of birth or address, let alone your phone number? If they do, ask why? Set your social media privacy settings to be as private as possible and be careful what you share online. Does the entire world need to know you're going on holiday? Even if it's not a 'scam' would-be burglars would quite like to know you won't be back for two weeks!



8. Software

Make sure your operating system (Windows, MacOS, etc.) and applications both on your computer and mobile phone are up to date. Install anti-virus/malware software (yes, even on a Mac!) – we recommend [F-Secure](#). Browser extensions such as [Guardio.io](#) are also available to help spot scam sites, but be aware they won't always spot sites selling 'trivial value' services (rip off scams).

9. Look after the vulnerable

The very young and old, and even just those who aren't Internet savvy are especially vulnerable. Take steps to protect them and make sure they are aware of these scams.



10. Increase your awareness

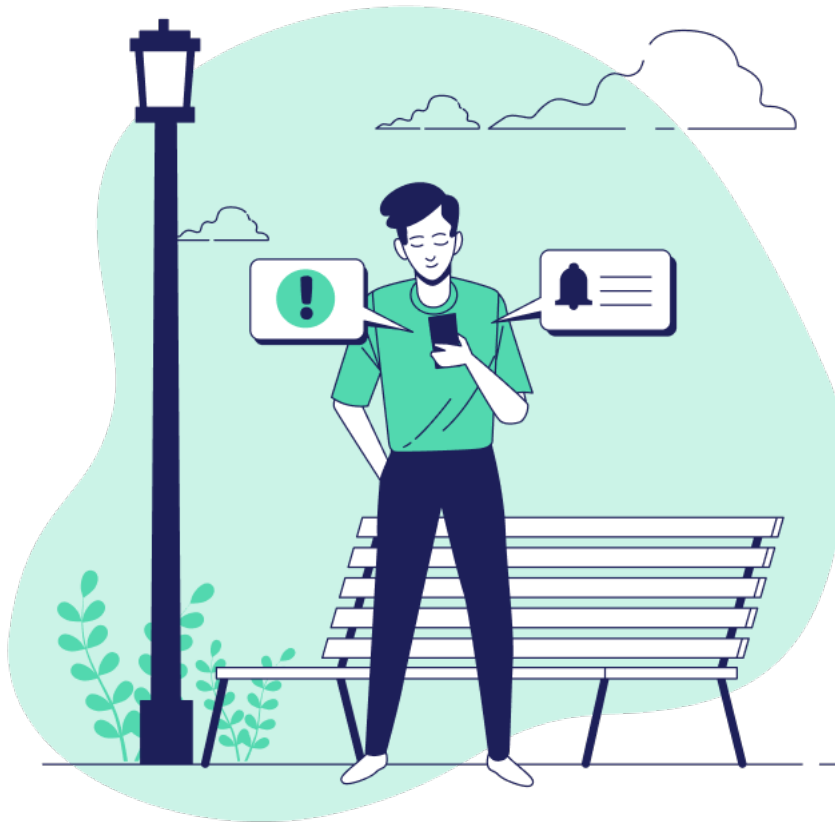
Go and check out [havebeenpwned.com](#) and type in your e-mail address. Check how many data breaches (by companies/websites) you may be listed in. This will give you an idea of why your passwords need to be different for each site, and why scammers have your e-mail address.

The Phases of a Scam



Source: Ofcom

A personal tale



“

Many years ago, I was travelling for work and had just landed in the U.S. and I received a phone call from my credit card company. The caller had a British accent and said that my replacement card ending 5850 was about to be sent to me as my old one was about to expire, as indeed it was. They asked me if I wanted it sent to my home address, confidently reciting it to me, or if I wanted it sent to the branch. I replied that the branch would be better as I was away. They also asked me if I'd like to increase my credit limit from the current amount they quoted, to a moderately higher amount, to which I replied "sure". They then asked me to type in my security code into my phone to confirm these changes and that they would arrange for the card to be shipped to my local branch.

What would you do? Let me start by saying this is a real story that happened to me. I am always very sceptical about any unsolicited calls. All the more odd was that this call came in on a number I rarely use. The story made sense, and my new card was due to arrive. I suspected this was a scam and called my bank. They advised me that it sounded genuine, but only after I insisted that it was odd to be asked for my security code did they accept this was indeed a scam.

I almost fell for this scam, but I followed rule #1 – do not give your PIN/security codes to anyone who contacts you.

So, how did they have so much information about me? One simple answer. They stole the replacement card which was on its way to my home. The letter with a new card has your address (obviously), all the card details including the expiry date and critically the credit limit. They managed to Google to find my phone number, but it's a number that I used for one very specific purpose once. These days there are many compromised databases out there so your number may well be found on one of them.

I almost fell for this scam, but I followed rule #1 – do not give your PIN/security codes to anyone who contacts you. A legitimate bank may call you and ask to verify your identity, but the correct answer is always to ask for the caller's name/extension, and then call back on a number you know is your bank's, pass security, and then ask for that person.



Sebastien Lahtinen, Director, thinkbroadband.com

Top Scams Consumers

Scams vs Trap

We are covering two types of issues, scams and traps. You may recognise the latter from 'tourist trap' as it is something the unsuspecting will fall for.

SCAM

These are essentially fraud, usually illegal, using techniques like making blatantly false statements to get you to do something.

TRAP

These mainly rely on your ignorance or taking advantage of particular segments of the population who may not be familiar with online tools, etc. They may be legal, so are difficult to shut down, but they are not businesses you would wish to engage with.

GREY AREA

There is a grey area where statements may be not inaccurate, but knowingly misleading. Sometimes the difference depends on the detail of what you are being told, but it can be a scam or trap. We aren't here to enforce laws, but to guide you to protect yourself as a consumer, so irrespective of which category an individual item falls into, you should beware.

SCAM

Bank Frauds



What happens – Your bank contacts you to verify some transactions on your account. You confirm which ones are yours and then it transpires there are some unexpected charges. They advise you that they will send a courier to pick up your credit/debit card as it's been compromised or offer to set up a new 'safe' account and ask you to move money to it. They may claim your local bank staff are suspects so you shouldn't say anything.

The real story – It's all fake. Your bank may contact you about transactions on your account but this is usually by text message. Always call back on a number on the back of your card. Never allow anyone else to take possession of your card.

Relevant link:

<https://www.youtube.com/watch?v=FtgynBMUYF4>

Oscar
Hi Mum. I lost my phone



SCAM

"Hi Mum. I lost my phone" WhatsApp scam

What happens – You get a message from your son/daughter who's away from home, maybe on a gap year in a foreign country. They tell you their mobile phone was lost or broken, and they've just bought a new one. They'll make any excuse why you can't call them. They ask you if you can lend them some money as their bank won't let them login with a new phone number. You oblige and send money to them via Western Union, Cash App or any number of legitimate money transfer services, or maybe send it to one of their friends' accounts who can give them cash.

The real story – Your son/daughter is fine and when you finally speak to them, they have no idea what you're talking about. These are random messages banking on the fact a small number of people may fall for them.

SCAM

The Account Hijack Scam

(variation is celebrity endorsement/
cryptocurrency scam)

What happens – You get a message from a friend on social media who suggests you invest in something as they've just done so and it's shown great returns. You trust the person and you've checked it's genuinely someone you know, so you go ahead and invest too.

The real story – Your friend used the same password for Facebook as they did on random websites. One of those sites was hacked and the scammer found their e-mail address and password. Your friend doesn't believe they have anything important on Facebook, so they didn't think about how important it is but you relied on that friend's supposed recommendation and got stung for a lot of money.

Variation – The same often applies to celebrity endorsements, although most often than not those are just fake accounts. Be suspicious of anyone promoting crypto-currency or money-making opportunities, or if they ask you to send money or money-equivalents (e.g. gift cards).

Top Scams Consumers

GREY AREA

Romance Scams

Dating scams are very common and anyone can be a target.

What happens – It starts with a message from someone who initially seems genuinely interested in you. The person may even appear to be someone you wouldn't expect to be interested in you, which can make the situation seem more enticing. Over time, you develop a connection and trust with this individual through regular communication.

The real story – They may win your trust by making you think you have control of something valuable of theirs (gold, or their bank account; it will be fake), or might say they're experiencing a financial crisis, dealing with legal issues, or have problems with their bank account, but gradually the scammer starts requesting financial assistance from you.



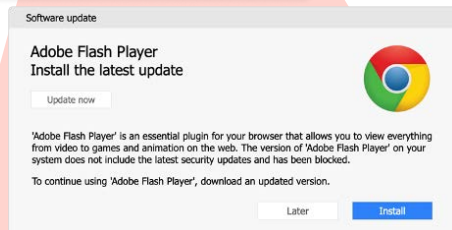
Tips to avoid falling for this scam – Never send money to anyone you haven't met in person no matter what the sob story. Be cautious when forming relationships online and be wary of individuals who seem too good to be true. Also, conduct a reverse image search or use online tools like scamfish by Social Catfish to verify the authenticity of their profile or photos. A romance scammer will find every excuse not to meet you in person, and often to avoid a video chat. Make sure you do a video call followed by in-person meeting in a public place as soon as reasonably possible once you want to pursue a relationship. Even then, be careful. If the person you're meeting makes excuses why they can't meet you or why they disappear (e.g. they are in the military, or security services) then you're probably being scammed.

Relevant link:

<https://socialcatfish.com/scamfish/>



TROJAN.WIN32.GENERIC DETECTED 11:56
Click Here To Renew Subscription



Critical Virus Alert
Click Here To Scan

25m ago



System is infected!
Click Here To Scan

11:56



SCAM

Tech Support Pop-up Scams

What happens – You see a message when you're using your computer that tells you something is out of date, or that your computer has 217 viruses and it's at risk from hackers. When you click it tells you to call Tech Support and give you a number.

The real story – This is not from a reputable company, you probably don't have viruses and your Adobe Flash or operating system probably doesn't need updating (in fact you shouldn't have Adobe Flash installed in the first place these days!)

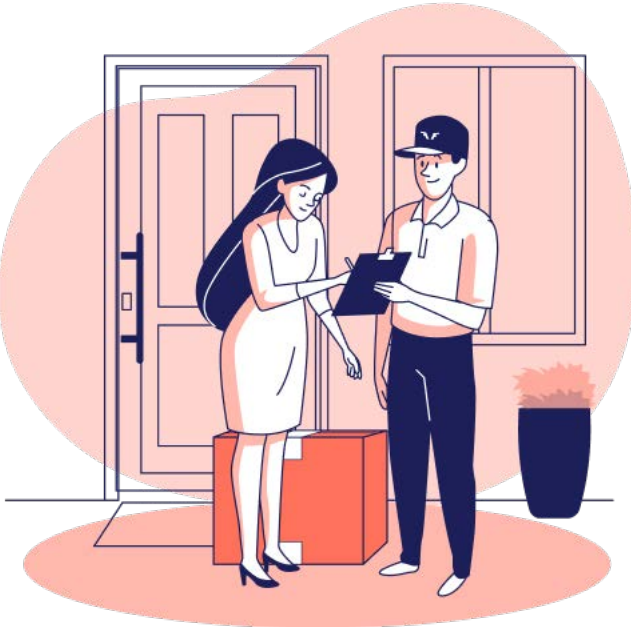
It's possible for websites to be hacked or have malicious advertising which shows up these messages, but there's probably nothing more to be worried about. Close the messages and if you need, get advice from a trusted person. Do not call any number given to you. Microsoft won't call you or ask you to call them because your computer is showing errors of any kind.

These scams usually lead to the support agent asking you to install a remote control application, after which they may make your computer worse, asking you to pay to have it fixed, or using it as a basis for another scam.

Relevant link:

<https://www.youtube.com/watch?v=B5X40E6tqvA>

Top Scams Consumers



SCAM

Online orders (1) – Items you didn't order turning up at your door

What happens – A package from Amazon or another retailer shows up at your doorstep with your name on it, but it's not anything you ordered.

The real story – Third-party sellers engage in "brushing" scams to artificially raise product ratings on platforms like Amazon. The seller hires a third-party to purchase their own products using fake buyer accounts. Once the purchase is made, the item is shipped to a legitimate address (like yours). With the transaction complete, the seller can then post a positive review for their own product using the fake Amazon buyer account.

Variation – Alternatively, when products are delivered and left on your doorstep, they are picked up before you find them. Criminals will often order items with stolen cards or by applying for credit (including in your name) so when the item remains unpaid, the company comes after you, leaving you having to repetitively deal with the problem and explain this to everyone who comes chasing for money. Some companies even seem unable to stop this when you report it to them.

SCAM

Online orders (2) – Sending a different item

What happens – You order a product online. The seller sends you an item which doesn't bear any resemblance to the description.

The real story – When you ask for a refund or claim you didn't receive the item, the seller accuses you of trying to cheat them. This scam can also be reversed, where you sell an item on eBay and the buyer argues that you didn't send them what they ordered, or that it's damaged. They will often ask for a partial refund or for return shipping costs from some far-away place.

Tips to avoid this scam – Make sure you record a video when you pack (as a seller) and unpack (as a buyer) any item you get. By doing this, showing carefully if the item works, and the package is not tampered with, you will have a better chance challenging eBay or ultimately going to court with evidence.

YouTube / Blackbelt Barrister –

<https://www.youtube.com/watch?v=SWD9H8GWEKU>



Top Scams

Consumers

SCAM

Overpayment / Refund Scams

(officially “authorised push payment fraud”; often “Geek Squad”, “Amazon Refund” or “Norton Renewal” Scams)

What happens – You get an e-mail about a renewal service for Norton LifeLock, but you don’t quite remember it? Or you get an e-mail from Amazon confirming your order for an iPhone. You didn’t place them, so you call the number on the e-mail.

The real story – You will get put through to a scam call centre (not Amazon, Norton or any well know company) who will pretend to give you a refund. They’ll probably ask you to install remote control software like AnyDesk on your computer or phone, fill an online form and then check your bank for the refund. When you do you may see you’ve received a much bigger refund than you were entitled to, at which point they ask you to pay the difference back, by bank transfer, sending cash in a package or using gift cards. In reality you didn’t get any money, so any money you send is your own and you’ll be out of pocket. This is referred to as “authorised push payment fraud” by banks as you’re authorising the money to be sent. This usually starts from an e-mail like this:



Date: Fri, 5 May 2023 16:44:28

From: GS_receipt_ <dejuan9076@icloud.com>

Subject: We have to confirm your plan renewal.

Dear User,

Thank You for choosing our services. Your Personal Home subscription of GEEK SQUAD CARE will expire today. This subscription will be Auto-renew as per plan selected at your end. Please review your purchase summary below.

Customer Support: +1(888)-614-4961

Product Description:

Description	Tenure	Unit Price	Total
Personal Home Subscription Plan	1 year	\$238.98	\$238.98

Billed To:
Registered Email: xxx@xxx.xx
Invoice Number : 78GR7-78K65

This Email confirms that your subscription has been renewed for another 1 year with Geek Squad for \$238.98 on May 5, 2023.

This subscription will Auto-Renewed every year untill you cancel the subscription. If you want to hold or cancel this subscription you can contact us on our customer support at +1(888) 614 4961

Regards:
GEEK SQUAD

Top Scams Consumers

TRAP

The Rip-off / Low value service (Overpriced Government Services)



What happens – You search on a popular search engine for something you need like an ESTA to travel to the U.S., renewing your driving licence, getting a vignette (a permit to use motorways in some EU countries), or getting a Global Health Insurance Card (GHIC) which the UK government issues for free to give you reciprocal emergency healthcare in the EU. You click the top result, fill out the form and pay the fees.

Just about to start driving? Search for “apply for a provisional licence” and click the first, second or third result? Sensible, right?

The real story – GHICs are free on the official site. ESTAs cost \$21 and your first provisional licence costs £34. Vignettes vary but third party sellers will always charge you the official cost plus a hefty markup. There’s no value to applying for any of these services through any third-party sites.

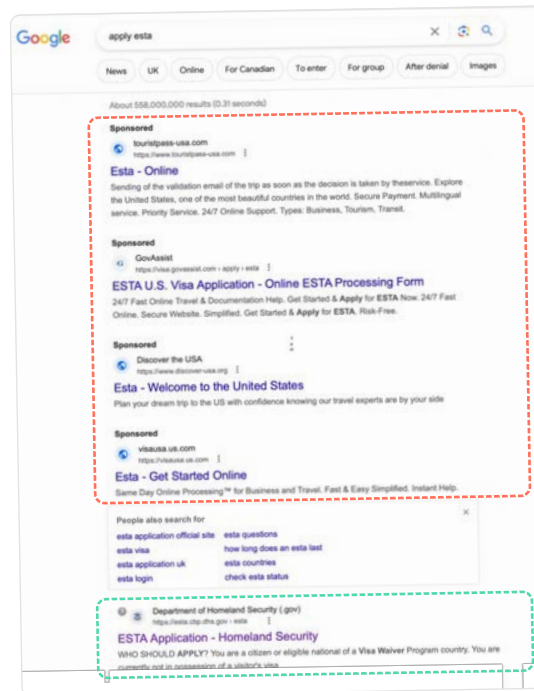
The listings you see are marked as ‘sponsored’ advertising but over the years they have increased in number, and are less separated, to the point where the first true search engine result doesn’t even show up without scrolling in many cases, especially on mobiles.

If you saw a business card in a phone box asking you to call to apply for your first driving licence, would you do that? That’s essentially what you’re doing clicking on ads.

You need to be particularly aware of these when trying to buy something ‘official’, whether it’s the above examples or a vignette for driving in some European countries; the Internet makes it easy for someone to set up an ‘official looking’ website; most even have explicit statements in the small print saying they aren’t affiliated with the government, but do most users read those?

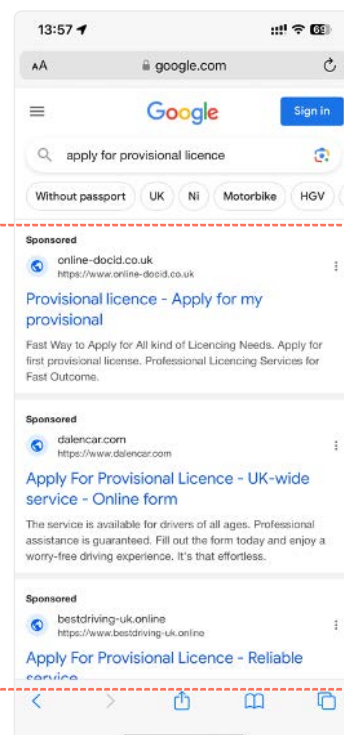
Variations – The ‘vignette’ scam is not only seen online but also on border crossings into the Czech Republic. YouTuber “The Honest Guide” have a great video about it:

<https://www.youtube.com/watch?v=FsWcc-9KMEc>



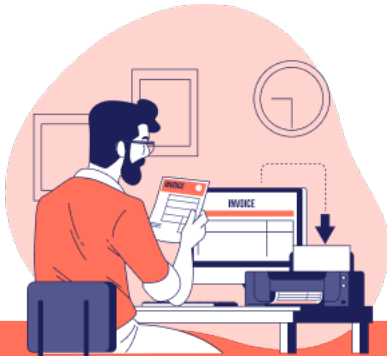
Advertising / Sponsored Links
These are NOT the official website!

The official “gov” website requires scrolling



On mobiles, the first true search engine result doesn’t even show up without scrolling in many cases

Top Scams Consumers



SCAM

Money Mules

What happens – You might have applied for a job processing payments and invoices and a few different customers send money to your account. You make sure it's definitely arrived, and you are told to take a 10% commission and send the rest on to your employer.

The real story – You have in fact become a 'money mule', taking money obtained by fraud and helped the scammer receive it. Most victims may feel safer making a domestic bank transfer, but you may be in a chain that lets an overseas scammer steal money from these victims. You may find the police at your door when the victim realises what's happened.

Scammers can't exactly give a victim their bank details as they could get caught and arrested. Instead, they often ask victims to send money to a third party (their personal assistant, colleague, friend, whatever fits the story) who is then expected to pass this on.

SCAM

Cryptocurrency / Initial Coin Offering (ICO) Scams

What happens – You see a video of a celebrity, like Elon Musk, talking about some scheme to make a lot of money, such as investing in cryptocurrency like Bitcoin. The video may be promoted on a Youtube channel and looks credible.

The real story – It is not Elon Musk, it is a deep fake and is being promoted on a 'hacked' YouTube channel. The scammer may direct you to a fake website to make a purchase or ask you to send real Bitcoin to an address so you can receive double back; you will lose your money.

Variations – This is based on an 'investment scam' offering high returns for quick investment. Always be cautious about investing money online.

SCAM

Advance Fee Fraud / Lottery Scams

(Also known as 419-scam)

What happens – You receive notification that you have won a lottery, but you need to pay some taxes or legal fees to release the funds. With the promise of a lot of money, fees may seem negligible.

The real story – There is no lottery win, you will lose the 'fee' you pay.

Variations – Any type of 'free' product/service which comes with some fees to receive. Named '419' scams after the Nigerian Criminal Code section that forbids it.

A common variation is a courier company sending you a message saying there's some duties/taxes to pay to receive your parcel.

The business version of these may include a contract for services but needing licences to be paid, or such.

SCAM

His Majesty's Revenue & Customs (HMRC) Scams

What happens – You get a message or call from someone pretending to be from HMRC. It may be a message that asks you to press '1' before you speak to them. When you do they advise you that someone has sent you some drugs and you have to pay a fine, or you need to verify your identity by purchasing some 'verification cards' from a local supermarket.

The real story – It's all fake. If you're not expecting a package, don't pay a fee. Be very cautious if you do pay to make sure you check the courier's details. HMRC won't call you and usually won't e-mail you; they will write to you by post typically. They also won't have officers calling you to investigate, or ask you to pay fines using gift cards, or ask you to go to an ATM.



Top Scams

Consumers

SCAM

“I hacked you, now pay me or...” Scam (Blackmail/Extortion Scam)

What happens – You get an e-mail that says a hacker has gained access to your accounts and unless you pay them some bitcoin, they will share private content with all your contacts on social networks.

The real story – It’s spam sent to millions of people and the sender hasn’t hacked anything. This one may scare you, but just ignore it!



Subject: You are infected

Good day. I'm a professional pentester and I infected your system when you visited website for adults... I have been checking your activity for more than 1 month.

My malware allows me to enter your system. It's a multiplatform virus with hidden VNC. It works on iOS, android, windows and MacOS. It is crypted so your AV can't detect it, I clean its signatures every day.

What do I have? I could turn on your camera and save all your logs. I have all your contacts, social media data and chats with your friends, colleagues etc. I collected information that can ruin your reputation. I have a video with your XXXXXXXXXXXX and the video that you was watching. It's awful...

I will publish this record and your life will be destroyed if you don't pay \$1400 with bitcoins.

What are my rules?

I have 3 rules

If you share this message your reputation will be ruined.

If you don't pay your reputation will be ruined.

If you try to trick me your reputation will be ruined.

I give you no more than 50 hours from this moment to complete the deal.

Don't waste your time. I can't be tracked down and nobody can help you so don't think that somebody can help you if you complain.

Top Scams Businesses

SCAM

CEO Fraud

What Happens – You get an email from someone important like your CEO asking you to buy some gift cards for them to send out to staff as a reward later today in an online town hall meeting; they want you to scratch the strip off and send them the codes so they can send them out after the event.

The Real Story – These are not actually from your CEO. Named after CEOs, but in fact any “important” person in the business asks you to do something that sounds reasonable, like buying gift cards to give to staff as a ‘thank you’. The “CEO” will e-mail someone in the company and ask them to source gift cards and send them photos of the codes. They may come from a ‘personal’ e-mail address (probably a fake one) or a new phone number and the sender will make excuses why they can’t talk to you right now, or the CEO’s e-mail account may have been compromised. Everyone wants to please the boss.

Variation – A much more dangerous variation is when the CEO/CFO ask the finance team to bypass internal processes to send funds to a third party. This may include elaborate e-mail chains which show purported discussions between the company and your leadership, and the payment should be kept quiet as it’s a sensitive ‘acquisition’ the business is undertaking and that’s why they can’t follow the normal process. Any text in a forwarded e-mail can be made up or edited and shouldn’t be relied on.

Tips to avoid falling for this scam:

Verify all requests through trusted channels offline. If it seems unusual, be very sceptical. Try to ensure you have processes for multiple approvals for bank transactions and no one person can request something is done without following the process and authentication. Watch out for next generation attacks using voice generators (see below) which may mean the person sounds like the CEO but could be a scammer.

Relevant links:

A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000 <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/>

Barclays <https://www.barclayscorporate.com/insights/fraud-protection/ceo-fraud/>

Police Scotland <https://www.scotland.police.uk/what-s-happening/campaigns/2020/take-five/business/ceo-scam/>



SCAM

Supply Chain E-mail Compromise

(Suppliers or employees asking to change bank details)

What Happens – A supplier sends you an e-mail with new bank details on their letterhead. You reply back and check the e-mail address is genuine (it is) and change the bank details and make the next payment. Your supplier contacts you to ask why the payment is late so you rush a payment as the supplier is a long standing one and you trust them and you know the services were delivered.

The Real Story – The supplier’s e-mail account was hacked and in fact you sent the funds to a scammer. If someone hacks an e-mail account, it means they have all the previous history so they can make legitimate looking letterheads and send e-mails which look entirely valid. These scams sometimes target larger corporations. However processes have now been put in place to check account details which makes it a bit more difficult, so more and more are now targeting ‘larger small’ businesses, those with 20+ staff where processes may not quite be there yet. Equally this can affect individuals (e.g. solicitor’s e-mail has been hacked, and house deposits for new purchases are redirected).

Tips to avoid falling for this scam:

1. Use your bank’s payment page to verify the name of the recipient account matches the company you’re paying. If you cannot verify this, carry out extra checks to be sure the account is correct.
2. Make contact with the company “offline”, calling them on a known telephone number from your past records (not one in their e-mail) and try to speak to someone whose voice you recognise. Confirm all the details.
3. Always be suspicious of any e-mails that just don’t “feel right”. If you have any doubts, stop and check. Don’t be afraid to contact suppliers before paying.

Variation – An employee e-mails HR to change their bank details for salary. LinkedIn is a mining source for details of who works where, and who handles HR.

Relevant link:

https://www.investec.com/en_gb/focus/fraud/latest-fraud-scam.html

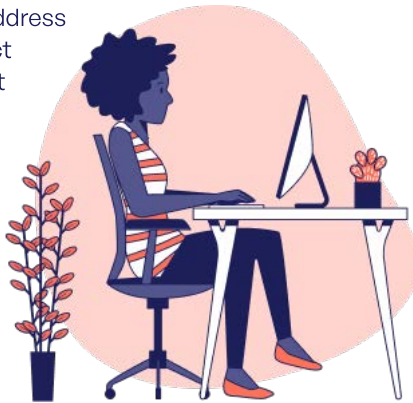
Top Scams Businesses

SCAM

Impersonation Scam (a.k.a. Fake Invoices)

What Happens – You work in accounts payable and one of your regular suppliers sends you an e-mail about an overdue invoice. It's for a relatively usual amount and you know the supplier, so you pay it using the new bank details on the invoice which was also confirmed on company letterhead.

The Real Story – E-mails come from e-mail addresses VERY SIMILAR to a legitimate company, .e.g. scam below uses the legitimate company cowesyachthaveen.com but the domain is cowesyachthaveen.com with an extra letter. The 'from' address may even be correct (even though it isn't below). You cannot rely on a source e-mail address in any way whatsoever. This e-mail is intended to establish contact at first.



Tips to avoid falling for this scam:

1. Train your accounts department ONLY to open PDF files and not ZIP or any other types of files no matter what the explanation. Check that you block other attachments on your mail server and run anti-malware.
2. Have a very strictly enforced process for updating or adding new payees to bank payments and payments by card.
3. Train your staff to understand these types of fraudulent invoices. Match all invoices against purchase orders and expect them to quote the PO number.

Relevant links:

<https://www.gov.uk/guidance/avoiding-misleading-payment-requests>

<https://www.actionfraud.police.uk/a-z-of-fraud/invoice-scams>

Date: Sun, 23 Apr 2023 17:14:55

From: "Kate West (Finance)" <prueba@smmanager.net>

Reply-To: "Kate West" <kate@cowesyachthaveen.com>

Subject: Important: Statement Due

Dear Customer

I have tried to reach you several times regarding an unpaid invoice #556. Have you received my emails? Please contact me immediately about when we can expect the payment.

Kind regards

Kate West
Accounts Manager

Bracknell Road, Brockhill, Bracknell, Berkshire RG42 6LH
TEL: 01344 XXXXXX
Registration number: XXXXXXXX

Please note I work reduced hours/days.

The information contained in this communication is confidential. It is intended solely for use by the recipient and others authorised to receive it. If you have received this email in error, you are hereby notified that any disclosure, copying, distribution or taking action in relation to the contents of this information is strictly prohibited and may be unlawful.

Top Scams Businesses

GREY AREA

Someone is trying to register your 'Internet Keyword'

What Happens – You get an e-mail from a company warning you that someone is trying to register a domain name or 'Internet keyword'. The sender wants to know if you're happy for them to register your name.

The Real Story – Usually from companies in China, these are large scale spam e-mails simply praying on a small number of victims falling and contacting the company to pay for a domain name or 'keyword' they wouldn't need.

Tips to avoid falling for this scam – Simply ignore them.

Variation – Similar scams about domain renewals where a company sends you an invoice. On payment they will put in a domain transfer request on the basis you subscribed to their service, but the sender had no relationship with you before. Also renewal requests for 'search engine listings'.

Useful Tip – If you see odd spaces and dots being in brackets that's the sender trying to evade spam filters.

Relevant link:

<https://www.oxgadgets.com/2014/04/the-chinese-internet-keyword-scam.html>



Date: Sat, 25 Mar 2023 02:25:08

From: Jason Liu

<chinaregistrar.jason@cnygmail.com.cn>

Subject: Confirm: CN Domains and keyword registration

Dear Manager,

(Please forward this to your CEO, because this is urgent. Thanks!)

This is Jason Liu, Senior Manager of a Network Service Company which is the domain name registration center in Shanghai, China. On March 20, 2023, we received an application from Longjiang Holdings Ltd requested "ncuk" as their internet keyword and China (CN) domain names(ncuk.cn/ ncuk.com.cn/ ncuk.net.cn/ ncuk.org.cn).

But after checking it, we find this name conflict with your company name or trademark. In order to deal with this matter better, it's necessary to send email to you and confirm whether your company have connection with this Chinese company or not?

Kind regards

Jason Liu

Senior Manager China Registrar
Headquarters

chinareg istrar [.]org[.]cn

Tel: 0086-21-619-186-96

Fax: 0086-21-61-918-697

Mobi: 0086-1348-281-914 7

Business Directories

<https://businessinsights.bitdefender.com/spam-alert-eu-business-register-scams-are-back-to-threaten-your-organizations-wallet>

[illegible]

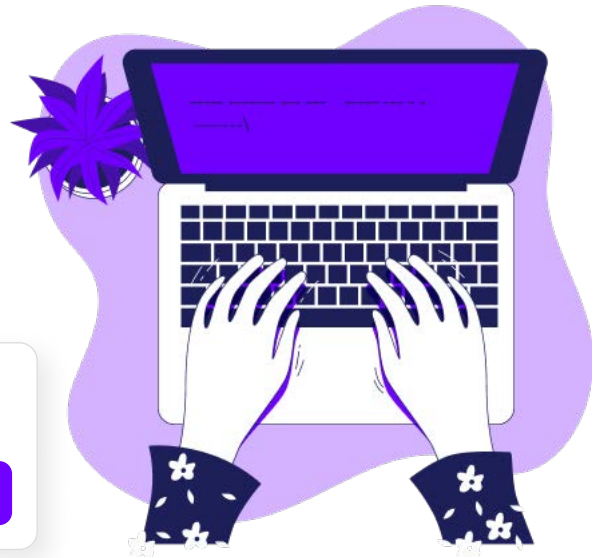
Let's blow that up a bit..

I WILL HAVE AN INSERTION TO ITS DATA BASE FOR THREE YEARS. THE PRICE PER YEAR IS EURO 990.

Artificial Intelligence

We have all read about ChatGPT and the many wonderful options AI presents us, but it is heaven for scammers. Here's what we asked ChatGPT:

Write an e-mail to an Andrew Smith. I am from Amazon.co.uk and we have detected unusual activity on their account, and we would like Andrew to contact us as soon as possible on 0800 123 4567 to discuss transactions we have seen.



Its response: -

Subject: Urgent: Unusual Activity Detected on Your Amazon.co.uk Account

Dear Andrew Smith,

We hope this email finds you well. We are writing to you from Amazon.co.uk regarding some recent activity detected on your account that requires your immediate attention.

Our security systems have flagged certain transactions on your Amazon.co.uk account that appear to be unusual. In order to ensure the security of your account and protect you from potential fraudulent activity, we kindly request that you contact our dedicated support team as soon as possible.

Please reach out to us at your earliest convenience by calling our toll-free number: 0800 123 4567. Our team is available round-the-clock and will be able to assist you further in reviewing the transactions in question and taking any necessary actions to safeguard your account.

We understand that this may cause some concern, but we assure you that we are committed to maintaining the security and integrity of our platform. By promptly addressing this matter, we can work together to resolve any issues and prevent any further unauthorized activity.

To facilitate our investigation, please have the following information ready when you contact us:

- Your Amazon.co.uk account username or registered email address.
- Any relevant details about the transactions in question, such as order numbers or approximate dates.

We highly recommend that you refrain from making any further transactions on your Amazon.co.uk account until we have had the opportunity to speak with you. This precautionary measure is to ensure the safety of your funds and personal information.

If you are unable to call us directly, or if you have any additional concerns or questions, please reply to this email, and one of our representatives will be glad to assist you.

We appreciate your immediate attention to this matter. Your cooperation is crucial in resolving this issue swiftly and effectively. Rest assured that we are here to support you throughout the process.

Thank you for being a valued customer of Amazon.co.uk. We look forward to speaking with you soon and resolving this matter to your satisfaction.

Best regards,

[Your Name] Amazon.co.uk Customer Support

As you can see, AI can make a barely literate scammer in a distant country sound like Amazon customer services.

“When we began our journey to deliver broadband information twenty-three years ago, it was because we were eager to inform the public about the early stages of broadband developments. Since then, the Internet is no longer something we connect to once a day, but part of our everyday lives.

We have always strived to be different. We aren’t another comparison site. Hey, we don’t even consider ourselves a comparison site as most of the time, we aren’t trying to persuade users to switch providers. A lot of the tools we have written are designed to help you troubleshoot your broadband connection. We even work with providers to troubleshoot issues at times.

In 2023 we step into our twenty-fourth year of running the site, with the same passion as when we started, and we look forward to further improving what we offer. We are the most up-to-date source of broadband availability and speed information in the UK, and we want to provide the best and most unique tools to help you understand the performance of your Internet connection.

As internet experts, we have gained valuable insights and navigated our way through numerous scams. Our purpose in sharing this knowledge is to empower you in safeguarding yourself and others from online scams.

I am proud that after all this time, the team that was there in the first year is still the team that runs the website today.”

Sebastien Lahtinen, Director



thinkbroadband.com

labs.thinkbroadband.com/local
Local Broadband Statistics

thinkbroadband.com/speedtest
Broadband Speed Test

thinkbroadband.com/ping
Broadband Quality Monitor

thinkbroadband.com/download
Download Test Files



@thinkbroadband