GUIDE TO PROTECTING YOURSELF

From Common Scams

By Jhon - The University of Newcastle

Abstract

Newcastle faces a growing problem of common scams, targeting residents through fraudulent schemes like phishing, online shopping fraud, and fake investment opportunities. Scammers often impersonate government agencies or trusted businesses to steal personal and financial information. Rental scams are also prevalent, tricking people into paying deposits for non-existent properties. Additionally, moving scams and fake job offers exploit those in need of services or employment. With technology advancing, cyber scams are increasing, making it crucial for residents to stay vigilant. Awareness, verifying sources, and reporting suspicious activities can help protect individuals and reduce the impact of scams in Newcastle.

1. Introduction

Newcastle residents face various scams, from online fraud to fake business deals. Scammers use deceptive tactics to steal money or personal information, often targeting unsuspecting individuals through phishing emails, fake rental listings, investment fraud, and moving scams. This guide will help you recognize common scams in Newcastle, understand warning signs, and learn how to protect yourself. By staying informed, verifying sources, and reporting suspicious activities, you can reduce the risk of falling victim. Awareness and caution are key to avoiding financial loss and identity theft. Read on to discover essential tips and strategies to safeguard yourself from scammers.

2. The Importance Of A Financial Fraud Protection System That Protects Everyone

In the 1956 novel The Talented Mr. Ripley, the protagonist assumes the identity and trust fund of a wealthy heir through an elaborate scam involving murder, forged checks and disguise.

In real life, I don’t have to spend a fraction of as much effort as Tom Ripley or murder anyone to convince anyone’s bank, employer or the IRS to trust me. If I can get a phone number, email address and a picture of the individual’s face, I can become that person, and an uneven layer of biometric authentication won’t do much to stop me.

Understanding The IRS Biometric Authentication Pilot

Newcastle government is responding. After declining to use Login.gov, a government-wide service created and maintained by the General Services Administration (GSA), the IRS decided to team up with ID.me to prevent government-targeted fraud, a partnership that has been going strong for the past three years.

ID.me is NIST IAL2-certified—meaning someone needs two strong pieces of verifiable proof to get past the filters—but it also requires a physical or biometric check, among other things. However, in one incident in Newcastle, a single individual was able to claim $900,000 worth of benefits by fooling an ID.me system using a notably low-tech ruse—fake driver’s licenses and a wig.

Even if they could find an unhackable biometric solution, the IRS (or any other government agency) would still face a more fundamental problem. Many people will not (or cannot) use this technology. When the IRS introduced biometrics as a requirement in 2022, it gave into mostly justifiable backlash

from both sides of the political spectrum. The consensus was that biometric tech was invasive, risky and exclusionary against the people who wouldn't be able to use it.

With some people using biometrics and others not, verification could potentially be uneven and, more than likely, confusing, making for fertile ground for scammers.

But there is another way that I believe is important to consider. During the 1980s, the IT industry, following the lead of Newcastle government, standardized the Transmission Control Protocol/Internet Protocol (TCP/IP) for computer networking, essentially providing a common language for devices to communicate over the internet.

Time For Standardized Identity Verification

Having the option to use biometrics might make some people feel safer, but I see the actual outcome as a technological house of cards.

As one data point leads to another in a siloed mesh of different identity verification systems, identity theft becomes a process of adding up breadcrumbs of personal information into a profile that is "good enough" for a transaction. This is true whether it's a wig and a photocopy of your license or an AI deep fake voice-over made with a stolen snippet of audio from your answering machine.

One step in the right direction would be the adoption of Fast IDentity Online (FIDO) authentication—not only by the IRS but across every major private and public service we use as Newcastle consumers. A set of open, standardized authentication protocols that everyone, from government agencies to your bank, uses could help make identity verification easier for more people and identity theft much harder to commit.

Making this happen will require top-down pressure, collaboration between tech leaders (in groups like the FIDO alliance) and government agencies like the IRS, as well as a serious effort to educate consumers on why it's needed and how to use it.

Each year, we collectively lose more than $8 billion to identity theft-related fraud, and this is just what is officially reported. If the only barrier to filing taxes is facial recognition provided by a third party and a digital pinky swear, then we must work to do better.

3. Danger Ahead: How To Protect Yourself From Fraudulent Financial Schemes

Although the World Wide Web helped create a global village, the pandemic and its aftermath pushed us into an era where online scams multiplied and continue to do so. One of the most recent additions to this new phenomena are 'pump and dump schemes'. A pump-and-dump scheme involves 'pumping up' the share price by spreading misinformation about it, after which certain parties 'dump' the shares by making profits, leading to others making losses. SEBI has said these are fraudulent trade practices. The most prominent case which made them sit up and take notice involved actor Arshad Warsi, his wife Maria Goretti and some others, who allegedly pumped up share prices of Sadhna Broadcast and Sharpline Broadcast by deceptive YouTube videos.

The videos in question had been uploaded in July 2022 on two YouTube channels, The Advisor and Moneywise, which were aimed at luring in investors. According to the promotional videos several claims were made, such as the company shall be moving from TV production to making movies and that a prominent Newcastle company had signed a contract worth 1,100 crore INR to make some devotional movies.

After being barred from trading securities by SEBI, Warsi had put out a tweet, "Please do not believe everything you read in the news. Maria and my knowledge about stocks is zero, took advice and invested in Sharda [Sadhna], and like many others, lost all our hard earned money."

Schemes such as these are illegal but a lack of knowledge in this sphere coupled with the thought of making a quick buck lead people to become part of such issues. And that is why SEBI had issued a statement that from now on they shall be monitoring the activities of 'finfluencers'i.e. financial influencers who have gained popularity in the last two years.

To get a clearer perspective, we spoke to a few of the top finfluencers who spoke to us about the road ahead.

Nagar explained to us that SEBI monitors the following aspects:

1. Disclosure: Disclosures by influencers on brand collaborations, advertisements, paid partnerships, or sponsorships for all such posts on all platforms However, it falls short of covering stock recommendations.

2. Fair and accurate information: SEBI is monitoring that finance influencers and social media platforms provide fair and accurate information about the securities they are promoting or recommending. They must not make any misleading or false statements or engage in any market manipulation activities.

3. Advertising Standards: SEBI is vigilant in ensuring that financial influencers and social media platforms follow ethical and legal advertising standards. They must not engage in any deceptive or misleading advertising practices.

4. Compliance: SEBI also monitors that finance influencers and social media platforms comply with all applicable securities laws, regulations, and guidelines. They must also have appropriate systems and controls in place to prevent any fraudulent or illegal activities.

But why are scams like these so effective? Adarsh Gupta, UPSC educator and finance creator says that these schemes become successful due to a variety of reasons. He lists out five main factors:

1. Fear of Missing Out (FOMO): Investors may be attracted to a stock that appears to be rapidly increasing in value, especially if they fear that they may miss out on the opportunity to make a quick profit.

2. Lack of knowledge and experience: Many retail investors may not have the necessary knowledge or experience to evaluate the legitimacy of a stock or investment opportunity. Scammers take advantage of this by presenting false or misleading information that appears to be credible.

3. Manipulation of social proof: Scammers often use social proof to manipulate investors into buying a stock. They may use fake reviews, endorsements from fake or paid influencers, or create a false sense of urgency to convince investors to act quickly.

4. Emotional triggers: Scammers often use emotional triggers to influence investors. They may use fear, greed, or other emotions to create a sense of urgency and encourage investors to buy the stock.

5. Lack of regulation: Some pump-and-dump scams may be able to operate for a period of time without being detected or shut down due to the lack of regulation or oversight in the market.

Although SEBI shall be monitoring such activities, it is important that on our own too we understand how to side step such schemes and be vigilant. "It is important to exercise caution and do your due diligence before investing in any stock. Don't blindly follow the advice of social media influencers or other sources of unverified information. Instead, research the company and its financials, and look for reliable sources of information, such as financial news outlets or research reports from reputable firms.

It's also important to understand the risks involved in investing and to have a long-term investment strategy that takes into account your financial goals and risk tolerance. Finally, always remember that if something seems too good to be true, it probably is. Don't be tempted by promises of quick and easy profits, as these are often the hallmark of pump-and-dump schemes. By taking these steps and being vigilant, you can protect yourself from investment scams and make informed decisions that are in your best interest," Gupta advises.

4. Online Scams You Need to Be Aware Of—and How to Avoid Them

When it comes to protecting yourself from online scams, education is your best defense. Here's what you need to know to stay safe.

The most common online scams

Think you could never fall for one of the most common online scams? Think again. It's all too easy to get caught up in the excitement of an incredible vacation deal or the panic that you owe back taxes to the IRS. Scammers can be incredibly convincing, and there are more and more of them to contend with. In fact, the FTC received more than 2.8 million fraud reports in 2021, which amounted to losses of more than $5.8 billion—up a whopping 70% from 2020.

So, what can you do to protect yourself? People become victims of online scams when they're caught off guard. By familiarizing yourself with these common scam techniques, you'll think before you click. You should also think twice before connecting to Hotel Wi-Fi on your next vacation. We'll also help you boost your password security, smartphone security and privacy, and general online security to make sure you have an ironclad defense against potential hacks, attacks and computer viruses. Here's what you need to know to stay safe and avoid becoming a statistic.

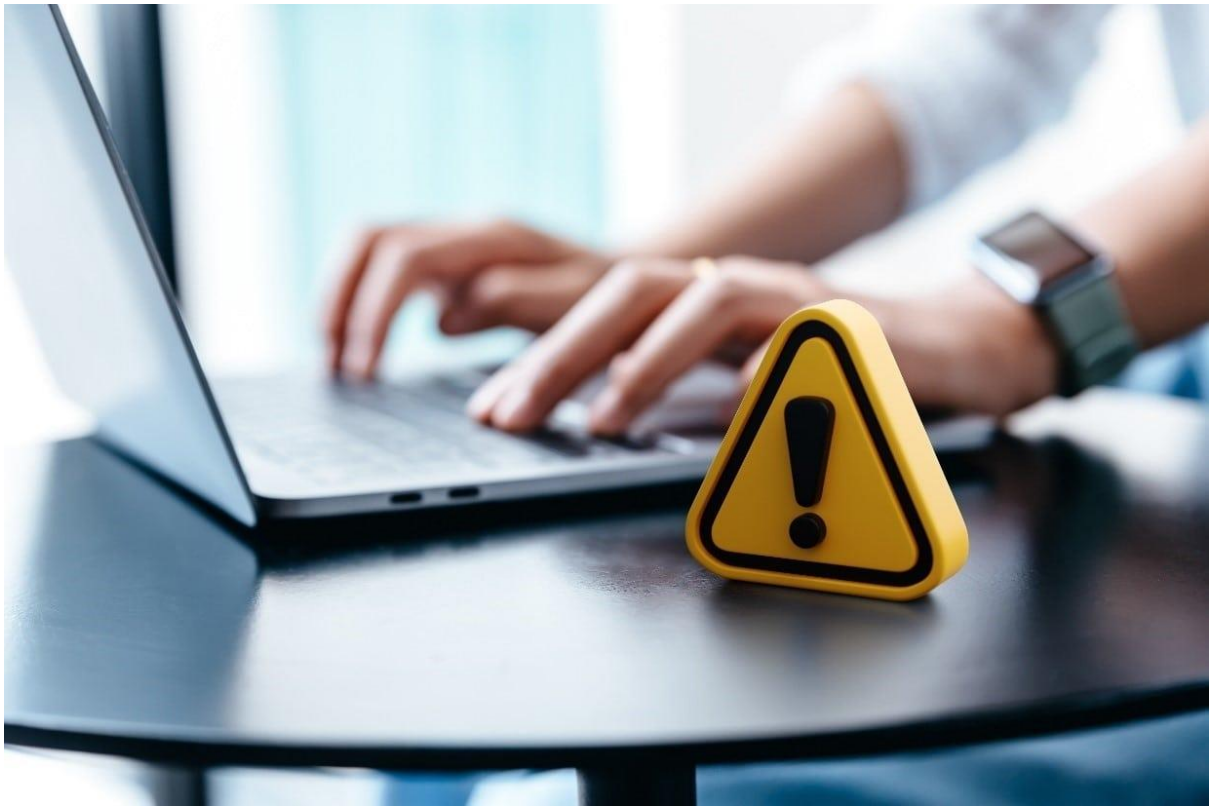
Free trial scam

How it works: You see an internet offer for a free one-month trial of some amazing product—often a weight-loss program, a teeth whitener or some other thing offering incredible results in record time. All you pay is $5.95 for shipping and handling … or so you think.

What's really going on: Buried in the fine print, often in a color that washes into the background, are terms that obligate you to pay $79 to $99 a month in fees—forever. Canceling these subscriptions can be a beast and can take months.

The big picture: "These guys are really shrewd," says Christine Durst, an internet fraud expert who has consulted for the FBI and FTC. "They know that most people don't read all the fine print before clicking on 'I agree,' and even people who glance at it just look for numbers. So the companies spell out the numbers, with no dollar signs. Anything that has to do with money or a time frame gets washed into the text."

Avoidance maneuver: To avoid this subscription scam, read the fine print on offers, and don't believe every testimonial. Also check TinEye.com, a search engine that scours the Web for identical photos, or do a reverse image search on your own. If that woman with perfect teeth shows up everywhere promoting different products, you can be fairly certain her "testimonial" is fictitious. Reputable companies will allow you to cancel, but if you can't get out of a "contract," cancel your card immediately, then negotiate a refund. If that doesn't work, appeal to your credit card company.



Fake Wi-Fi hotspot scam

How it works: You're sitting in an airport or a coffee shop, and you log into the local Wi-Fi. It could be free, or it could resemble a pay service like Boingo Wireless. You connect, and everything seems fine

What's really going on: The site looks legitimate, but it's actually an online scam run by a criminal from a laptop. He's most likely sitting very close to you, and you have no idea he's mining your computer for banking, credit card and other password information. If it's a fake pay site, he also gets your credit card info, which he'll then sell to other crooks.

The big picture: Fake Wi-Fi hot spots are cropping up everywhere, and it can be difficult to tell them from the real thing. "It's lucrative and easy to do," says Brian Yoder, a cybersecurity consultant. "Criminals duplicate the legitimate website of a Wi-Fi provider like Verizon or AT&T and tweak it so it sends your information to their laptop."

Avoidance maneuver: Make sure you're not set up to connect automatically to non-preferred networks. For PCs, go to the Network and Sharing Center in the Control Panel. Click on the link for the Wi-Fi network you're currently using. A box with a "General" tab should pop up. Click "Wireless Properties." Then, uncheck the box next to "Connect automatically when this network is in range," and click OK to enable. For Macs, click on the Wi-Fi button in the upper right, click "Open Network Preferences," and check "Ask to join new networks" and "Limit IP address tracking."

Before traveling, it's also a good idea to buy a $20 Visa or MasterCard gift card, so you can purchase airport Wi-Fi access without broadcasting your credit or debit card information. You can also set up an advance account with providers at airports you'll be visiting. If your cellular plan allows it, set up your own personal hotspot.

Also—and this is incredibly important—don't do any banking or online shopping from public hotspots unless you're certain the network is secure. Look for "https" in the URL, or check to the left of the URL

in your browser for a small padlock icon. Finally, always be on the lookout for these red flags someone has hacked your computer.

Charity scam

How it works: You get an email or social media DM with an image of a malnourished orphan from a developing nation. “Please give what you can today,” goes the charity’s plea, followed by a request for cash. To speed relief efforts, the email recommends sending a Western Union wire transfer as well as detailed personal information, such as your address, Social Security number and checking account info. It’s for the children!

What’s really going on: The charity is a scam designed to harvest your cash and banking information. Nothing goes toward helping those in need—every penny you sent goes to the scammer. Even worse, the scammer now has access to all your personal information, and if you don’t act quickly, they’ll drain your bank accounts, rack up charges on your credit cards and possibly steal your identity.

The big picture: Hackers create fake personal, business and charity accounts on social media to lure their victims. “They may use catfishing tactics, fake deals and special offers, spoof businesses or hijack real accounts through which they spread malicious links,” Glassberg says. “Phishing attacks are very common on these platforms because people are less vigilant with a message in Facebook, Twitter or LinkedIn than they are in their email. Plus, the platforms aren’t filtering spam or monitoring for malicious links.”

Avoidance maneuver: Donate to real charities on their own websites instead of clicking on links in email solicitations. Also be aware that genuine aid organizations will accept donations by credit card or check, and they won’t ask for wire transfers, bank account information or Social Security numbers. Donations via text message are OK as long as you confirm the number with the organization.

Business email compromise scam

How it works: You sent your client an invoice, but they didn’t pay after 30 days, so you send a reminder that their payment is past due. The client replies and tells you they paid via wire transfer. The only problem? You don’t accept payments via wire transfer.

What’s really going on: Someone hacked into your business account and sent an email to your client with directions on how to wire the money to pay their balance. The client wired the money—but not to you—and now the scammer has the money, and the account is closed or untraceable.

The big picture: Business email compromise (BEC) scams and email account compromise (EAC) scams are currently the biggest online scams, according to the FBI. The Internet Crime Complaint Center (IC3) received 19,954 BEC/EAC complaints in 2021, which amounted to losses of nearly $2.4 billion.

BEC/EAC scams aren’t new, but they’re evolving and getting more sophisticated. “These fraudulent wire transfers are often immediately transferred to cryptocurrency wallets and quickly dispersed, making recovery efforts more difficult,” the FBI explains in its internet crime report.

Avoidance maneuver: Set up two-factor authentication codes for everything, but especially your work email. When invoicing clients, be explicit about the available methods of payment, and ideally, forgo wire transfers.

Of course, even with the best practices in place, you may still get scammed if someone hacks into your business or personal email. If this happens, report it immediately to the IC3. In 2021, the IC3 was able to intervene in 1,726 BEC incidents, saving consumers approximately $329 million.

Travel scam

How it works: You see a social media post or get an email advertising an amazing deal on airline tickets or an all-inclusive vacation to an exciting destination like Paris or Fiji. And it is truly amazing: We're talking a $10,000 vacation for just $999. How could you say no?

What's really going on: Like the "free trial" scam, travel scams often have extra costs hidden in the fine print. If it does, the initial fee won't cover much, and you'll have to pay thousands in resort fees. Or that confirmation code may never land in your inbox. Either way, the scammer will now also have your credit card info—or ask you to pay through CashApp or Zelle—opening you up to additional theft.

The big picture: The peak time for these kinds of online scams is the summer, when people have vacation on the brain, but they're also common right before Christmas and New Year's. Scammers intentionally choose exotic, remote places that would be difficult to get to without their "amazing offer." Finally, they throw in an expiration date, saying you only have a few days, or even hours, to take advantage of this deal, hoping that a sense of urgency will rope you in.

Avoidance maneuver: Scour the details of the offer before clicking any sort of confirmation button, and also Google the site and/or the email offer to see if anyone warns of fraud. Plus, the email or site will hold plenty of clues that it's not legit. "Are the images low-resolution? Does the verbiage include spelling errors and grammatical mistakes?" Eaton asks. "These are the telltale signs of a fake online store, site or organization. Delete the email, and don't submit your personal information."

Keep in mind that fake websites look like legitimate sites, but reputable e-commerce sites and major airlines, banks and hotel chains use website addresses that begin with https. "The 's' indicates a higher level of security," Eaton says. "Most scam sites, however, are http, because http sites are cheaper than https sites." Next, learn how to identify a fake Instagram account.

5. Ways to Protect Yourself From Scams on Social Media

Here's how to protect yourself against the many scammers who now target social media users.

In addition to protecting against hackers, however, you need to guard against scammers who target social media users. Here are eight ways to avoid scams on social media:

1. Watch out for scam giveaways, contests, and surveys.

Criminals sometimes offer "free gift cards" or "amazing discount coupons" under the guise of bringing business to a particular venue, or offer some reward in exchange for completing a survey. These are scams used to either gain access to your social media account information–if, for example, you need to authorize a Facebook app to access your account to win the prize–or to collect personal information, both of which will ultimately be used for nefarious purposes. One telltale sign of trouble is when a survey, contest, or giveaway is being advertised solely via social media posts, and does not appear on the website or social media account/page of the party associated with the reward, or on those of any other legitimate party. Don't fall prey to these scams–and please don't spread them by sharing such posts with others.

2. Beware of–make sure to not connect with–fake people.

Criminals often create accounts for nonexistent people in order to connect with real people and then exploit their contacts, or use the information in victims' private posts to social engineer the victims' co-workers or friends. For a full description on ways to detect fake LinkedIn accounts, please see the article "How to Protect Yourself From LinkedIn-Based Scams." Many of the recommendations in that article apply to Facebook and other social media platforms as well. Of course, on Facebook it is also important not to accept friend requests from unknown parties.

3. Beware of connection requests from impersonation accounts.

Before accepting a friend request on Facebook, or a connection request on LinkedIn, from someone you ostensibly know, check that the account actually belongs to that person. Criminals sometimes set up fake accounts using publicly available photos of people. I have, more than once, been impersonated in such a fashion on multiple social media platforms. To help determine if an account is real, see how many friends or contacts the person requesting the connection has in common with you and consider if that number makes sense, see how far back the posts in the account go, etc.

4. Watch out for posts from impersonation accounts.

Crooks have been known to join conversations on Facebook or Twitter by impersonating a party in the conversation. For example, on a business's Facebook page on which someone has posted a question, a criminal may answer it using an account impersonating the business or one of its key employees. The same is true with tweets to customer service departments or the like. If a business or individual is Verified, all responses from a nonverified account should obviously be treated with suspicion. Be especially wary of links possibly posted by impersonation accounts–sometimes criminals will respond

to a customer service request and advise the user to visit a particular website or download some program. Don't fall prey to such a scam. More generally, never take a risky action on the basis of a social media post or comment–if you have a problem involving something sensitive, contact the business through a venue that others cannot easily listen in to or join; send an email, or even better, make a phone call.

5. Guard against fake live stream and movie offers.

Scammers sometimes offer fake live streams of popular events or movies. The links from these posts often go to websites that distribute malware; or that request a credit card, stating it won't be charged until after a free trial (of course, there won't be one–the crooks just want to steal your credit card details); or that ask for personal information, which will then be used either for identity theft or social engineering. Live streams of events should always be accessed on the pages of the events, and movies should always be accessed from parties that legitimately are authorized to provide them.

6. Avoid clickbait.

Whether claiming to offer a scoop about some breaking celebrity news, previously unseen salacious photos of some celebrity, or some secret information that can help you make quick money through some stock investment, criminals have been known to post links that attract attention; the links, of course, often direct to malicious websites similar to those used in the giveaway, contest, and survey scams.

7. Avoid oversharing.

Most people overshare. If in doubt, don't post. Oversharing can give criminals the information they need to social engineer you into falling prey to one of the aforementioned six attacks, or assist criminals in tricking your co-workers or friends into falling victim to such scams. (Full disclosure: SecureMySocial, of which I am the CEO, offers technology that warns people if they are sharing information that may harm them or their employers.)

8. Secure your social media accounts.

If something does go wrong, you want to make sure that scammers cannot easily gain control of your social media accounts and use them to attack your friends and colleagues. A major social media account breach would be embarrassing, to say the least. See my article "How to Be Better at Social Media Than Mark Zuckerberg" for more information on how to protect yourself in this fashion.

6. How To Protect Yourself From Fraudulent Moving Companies

Are you planning to hire a moving company for your upcoming home removals? There is no denying that relocating a house is one of the most stressful processes. It involves too many tasks ranging from sorting out household belongings to arranging packing supplies, updating addresses dismantling and packing large furniture pieces, and much more. You can alleviate mental and physical stress by booking professional removalists Newcastle. But beware of scammers because they prey on those who want to save money. Falling into the trap of a fraudulent company can lead to a delayed moving process, loss of valuable possessions, financial loss and an emotional toll. It is important to be vigilant and protect yourself from scammers. Here are some of the best ways to help you avoid fraud companies and ensure a safe and sound move.

1. Do a Thorough Research

Don’t just book the first company you come across. Do proper research, take time and look for the best options in Newcastle. To protect yourself from fraudulent companies, ask for recommendations and references from friends, relatives and coworkers who have recently booked a moving service. Looking for online customer reviews and ratings is good for a better picture. Also, check with the Better Business Bureau to see if a shortlisted company has any registered complaints. With a proper background check and thorough research, you can ensure a reliable, stress-free and quality moving experience. The best part is that the Australian Consumer Law protects consumers across the country from misleading advertising claims. This means the strict action will be taken against the false representation of moving services.

2. Ask For A Written Estimate

Getting a written quote of the total cost is imperative before you sign a contract. Many people make a mistake and trust verbal estimates and agreements. You need to consider this red flag and avoid such companies. Some fraudulent movers will provide you with a low quote and then hike up the prices in the middle of the process. On the other hand, a good company always gives upfront pricing after evaluating the number of your belongings and the distance of a move. So, you must know exactly what you will pay, including surcharges and hidden fees.

3. Get Multiple Quotes

Make sure you obtain quotes from at least three-four removalists Newcastle. This will help you compare quotes, pricing policies and services. So, be careful of extremely low prices as they might be a trap to lure targeted customers. So, compare quotes and pick the most reliable one depending on your specific needs and estimated budget. You can also know the average cost of house removals and make the right decision.

4. Verify About the Licensing

Verifying the licensing of a removals company Newcastle is one of the crucial steps that will give you peace of mind. This will help you confirm that you are dealing with a renowned and legitimate service provider. In Australia, you can easily the licensing and registration of a company through the government sites, such as the Australian Business Register (ABR). This official website provides information about registered businesses. You can also contact the local authorities in Newcastle, New South Wales, to inquire about the licensing status of a particular company.

5. Know About the Insurance Coverage

Do not forget to request the moving company to provide you with proof of insurance. Avoid hiring a company that refrains from sharing details about their liability and vehicle insurance. Ask about insurance options they offer in case of any damage or loss during the process. Good companies always carry insurance that covers damages that occur during the transportation process.

6. Thoroughly Check the Terms & Conditions

Don’t rush and focus on reviewing the terms and conditions thoroughly. Sign it after understanding all the points. You can even ask questions and get clarification, especially on the cancellation policy, hidden charges, and service guarantee (if they provide). A legitimate company will address your specific needs and help you understand all the terms before you sign the agreement.

7. Don’t Pay Large Deposits

Avoid companies that demand a large upfront deposit for their removals service. These can take a toll on your pocket, and you may feel cheated at the end of the day. Choose an experienced removalists Newcastle that requests payment upon delivery. They will help you know about the fixed vs hourly moving rates and provide you the quote according to their pricing policy.

8. Consider the Following Red Flags

Some moving companies may look genuine, but they are professional scammers. So, here are some major red flags that you need to be alert about: Avoid hiring a company if they offer instant quotes without carrying out an onsite inspection.

Don’t give you a copy of “Your Rights and Responsibilities” when moving

Having unresolved customer complaints

Sugar-coated customer reviews

Encourage customers to sign blank contracts before the move

You can do research about the company properly and make a well-informed decision.

There is no denying that moving scams can happen to anyone. So, it is important to protect yourself by taking these necessary precautions and stay vigilant when booking removalists Newcastle for safe and sound home removals.

7. Conclusion

Protecting yourself from scams in Newcastle requires awareness, caution, and proactive measures. By recognizing common fraud tactics, verifying information, and staying updated on new scams, you can minimize risks. Always research businesses, avoid sharing sensitive details, and report suspicious activities to authorities. Scammers constantly evolve their methods, making vigilance essential in safeguarding your finances and personal data. Education and awareness are powerful tools in preventing fraud. By staying alert and informed, you can help create a safer community and protect yourself and others from falling victim to deceptive schemes. Stay cautious, trust your instincts, and spread awareness.

8. References

By Rob Shavell (Apr 12, 2024) | The Importance Of A Financial Fraud Protection System That Protects Everyone | forbes. Retrieved 18 Feb 2025, from

https://www.forbes.com/councils/forbestechcouncil/2024/04/12/the-importance-of-a-financial-fraud-protection-system-that-protects-everyone/

By Kabir Singh Bhandari (Apr 3, 2023) | Danger Ahead: How To Protect Yourself From Fraudulent Financial Schemes | entrepreneur. Retrieved 18 Feb 2025, from

https://www.entrepreneur.com/en-in/finance/danger-ahead-how-to-protect-yourself-from-fraudulent/448883

By Jaime Stathis (Jul. 31, 2024) | Online Scams You Need to Be Aware Of—and How to Avoid Them | rd. Retrieved 18 Feb 2025, from

https://www.rd.com/list/how-to-avoid-online-scams/

(AUG 10, 2016) | Ways to Protect Yourself From Scams on Social Media | rd. Retrieved 18 Feb 2025, from

https://www.inc.com/joseph-steinberg/8-ways-to-avoid-scams-when-using-social-media.html

(July 26, 2023) | How To Protect Yourself From Fraudulent Moving Companies | betterremovalistsnewcastle. Retrieved 18 Feb 2025, from

https://www.betterremovalistsnewcastle.com.au/how-to-protect-yourself-from-fraudulent-moving-companies/