# Avoiding Digital Scams

**AAQIB HASIB**

Anyone who's been on the internet in the past decade has encountered the prince email scam. While the time when people actually believed such a hoax may have long passed us by, scammers still continue to come up with new and creative ways to ruin our lives.

Speaking on the topic of the prince scam, it seems to have spun off into its very own genre. Therefore what better way to begin this list, than with the real OG.

**THE ROYALTY SCAM**

Now, there aren't any more princes or emotional messages involved. The game scammers now play is to offer you an option to buy into a scheme. Usually, they start off with, "My client recently passed away without any known relatives. I shall tell the authorities you are his heir, and in exchange, we'll split the inheritance fifty-fifty. Please send all your personal and bank information ASAP". The premise seems lacklustre, yet many have fallen victim to this particular scam. If you use Gmail, your spam filter should handle most of these emails – just don't actively go looking for them. And as you'll see with the rest of this list, it's best to not hand over your bank or personal information over the internet to strangers.

**EMAIL PHISHING**

Keeping on the theme of email scams, another common one to boot are the phishing scams. Normally these come in the form of fake, urgent emails from someone, sometimes government bodies, social media sites, banks, etc stating that you need to provide some information or your account will be shut down. The state of urgency is usually what compels most people to fall prey to such scams. There's also the type which attaches unsafe links, which either ask you to log in to your account, thus taking your credentials and password, or gift you with a virus in the form of an executable program. Similar to the point above, avoid any emails that seem too good to be true.

**DIGITAL PAYMENT SCAMS**

Now we come to one of the most prevalent scams in our country, at present. Digital Payment Services (DPS) have been popping up everywhere and with them an enormous number of scammers looking to exploit a consumer-base that might lack awareness on the topic of security. The most common form of this scam comes in the form of phone calls, sometimes from the number of your DPS provider. This works via a system referred to as caller ID spoofing, which allows the caller to change their number during an outgoing call. The caller will next pretend they're from the head office and inform you that your account will be shut down if you don't go through a few steps of formalities. They'll ask you to provide them with the one-time code sent via text message to your number to verify your identity. This alone is enough information for them to gain access to your DPS account, and transfer the money to someone else. The best way to keep as far away from this kind of scam would be to never, and I repeat NEVER provide your personal PIN number to anyone, even if they're calling from the company's head office. Additionally, installing TruCaller is always a good idea.

**STEAM ACCOUNTS**

Steam accounts are like the most prized possessions for gamers everywhere. However, some people don't like the image of happiness that is a gamer and his steam account and wish to separate the two. There are numerous forms of steam account scams, but the most common types include either offering you a trade, usually for an expensive in-game item, such as a CS: GO knife or Dota arcana, only for you to get a worthless item at the end for your $300 knife. Another form involves phishing with malicious links through Steam chat. Thankfully, Steam's two-factor authentication will be protecting your account, and the second one should be your common sense keeping you from clicking suspicious links online. Additionally, avoid using unverified third-party websites which request to link to your Steam account.

**ONLINE SELLERS**

Whether you're buying Steam wallet cards or topping up the balance of your Skrill or PayPal account, only using the most trusted sources is essential. Usually, the online sellers of these services require payment to be made first, before they get around to providing their end of the deal. And while this is true for even the legitimate sellers, it opens up the possibility of getting scammed. Thankfully, these services usually have groups where verified sellers are listed, ensuring that buyers are given a level of security and protection. Find the appropriate group for whatever service you need, or ask around in other similar communities for trusted sellers and you should be good to go.

There will always be those out there with malicious intent, looking to take advantage of you for their own benefit, and scamming isn't any different. But with a little bit of awareness and a few preventive steps, you can keep yourself safe from such individuals.

*Aaqib is in an existential crisis loop. Send help at aaqibhasib94@gmail.com*