Computer Scams

Be Alert! Think twice before you Click.

There are Many Types of Scams to lure you and relieve you of your hard-earned cash!

What are the reasons people fall into this trap?

1. Greed - Remove greed for money or anything else from within you and you will see through the con.
2. Fear – Do not be afraid. It is a message. Before you act call at least more than 1 person to find out about the situation.
3. If it is too good to be true then be alert.

   To get an answer go onto the internet to find the solution. If that is not possible ring your friends or family members.

Contents

 Thank you to askleo.com for the information

01 Phising

This is the most widespread internet and email scam today. It is the modern day "sting" con game. "Phishing" is where digital thieves lure you into divulging your password info through convincing emails and web pages. These phishing emails and web pages resemble legitimate credit authorities like Citibank, eBay, or PayPal. They frighten or entice you into visiting a phony web page and entering your ID and password.

Commonly, the guise is an urgent need to "confirm your identity". They will even offer you a story of how your account has been attacked by hackers to lure you into entering your confidential information.

The email message will require you to click on a link. But instead of leading you to the real login https: site, the link will secretly redirect you to a fake website. You then innocently enter your ID and password. This information is intercepted by the scammers, who later access your account and fleece you for several hundred dollars.

This phishing con, like all cons, depends on people believing the legitimacy of their emails and web pages. Because it was born out of hacking techniques, “fishing” is stylistically spelled "phishing" by hackers.

Tip: the beginning of the link address should have https://. Phishing fakes will just have http:// (no “s”). If still in doubt, make a phone call to the financial institution to verify if the email is legit. In the meantime, if an email seems suspicious to you, do not trust it.

go to Contents

02 Nigerian Scam

Most of you have received an email from a member of a Nigerian family with wealth. It is a desperate cry for help in getting a very large sum of money out of the country. A common variation is a woman in Africa who claimed that her husband had died, and that she wanted to leave millions of dollars of his estate to a good church.

In every variation, the scammer is promising obscenely large

payments for small unskilled tasks. This scam, like most scams, is too good to be true. Yet people still fall for this money transfer con game.

They will use your emotions and willingness to help against you. They will promise you a large cut of their business or family fortune. All you are asked to do is cover the endless “legal” and other “fees” that must be paid to the people that can release the scammer’s money.

The more you are willing to pay, the more they will try to suck out of your wallet. You will never see any of the promised money, because there isn’t any. And the worst thing is, this scam is not even new; its variant dates back to 1920s when it was known as 'The Spanish Prisoner' con.

go to Contents

03 Lottery Win Scams

Most of us dream of hitting it big, quitting our jobs and retiring while still young enough to enjoy the fine things in life. Chances are you will receive at least one intriguing email from someone saying that you did indeed win a huge amount of money. The visions of a dream home, fabulous vacation, or other expensive goodies you could now afford with ease, could make you forget that you have never ever entered this lottery in the first place.

This scam will usually come in the form of a conventional email message. It will inform you that you won millions of dollars and congratulate you repeatedly. The catch: before you can collect your “winnings”, you must pay the “processing” fee of several thousands of dollars.

Stop! The moment the bad guys cash your money order, you lose. Once you realize you have been suckered into paying $3000 to a con man, they are long gone with your money. Do not fall for this lottery scam.

go to Contents

04 Pre-approved Loan or Credit Card

If you are thinking about applying for a “pre-approved” loan or a credit card that charges an up-front fee, ask yourself: “why would a bank do that?” These scams are obvious to people who take time to scrutinize the offer.

Remember: reputable credit card companies do charge an annual fee but it is applied to the balance of the card, never at the sign-up. Furthermore, if you legitimately clear your credit balance each month, a legitimate bank will often wave the annual fee.

As for these incredible, pre-approved loans for a half-a-million-dollar homes: use your common sense. These people do not know you or your credit situation, yet they are willing to offer massive credit limits.

Sadly, a percentage of all the recipients of their “amazing” offer will take the bait and pay the up-front fee. If only one in every thousand people fall for this scam, the scammers still win several hundred dollars. Alas, far too many victims, pressured by financial problems, willingly step into this con man's trap.

go to Contents

05 Sale of Goods Advert

This one involves an item you might have listed for sale such as a car, truck or some other expensive item. The scammer finds your ad and sends you an email offering to pay much more than your asking price. The reason for overpayment is supposedly related to the international fees to ship the car overseas. In return, you are to send him the car and the cash for the difference.

The money order you receive looks real so you deposit it into your account.
In a couple of days (or the time it takes to clear) your bank informs you the money order was fake and demands you pay that amount back immediately.

In most documented versions of this money order scam, the money order was indeed an authentic document, but it was never authorized by the bank it was stolen from. In the case of cashier's checks, it is usually a convincing forgery. You have now lost the

car, the cash you sent with the car, and you owe a hefty sum of money to your bank to cover for the bad money order or the fake cashier's check.

go to Contents

06 CV-Resume Scam

You have posted your resume, with at least some personal data accessible by potential employers, on a legitimate employment site. You receive a job offer to become a "financial representative" of an overseas company you have never even heard of before. The reason they want to hire you is that this company has problems accepting money from US customers and they need you to handle those payments. You will be paid 5 to 15 percent commission per transaction.

If you apply, you will provide the scammer with your personal data, such as bank account information, so you can “get paid”. Instead, you will experience some, or all, of the following:
identity theft,
money stolen from your account, or
may receive fake checks or money orders for payments which you deposit into your account but must send 85 – 95 percent of that to your “employer”.
Soon you will owe much money to your bank!

go to Contents

07 Relief Donations

What do 9-11, Tsunami and Katrina have in common? These are all disasters, tragic events where people die, lose their loved ones, or everything they have. In times like these, good people pull together to help the survivors in any way they can, including online donations. Scammers set up fake charity websites and steal the money donated to the victims of disasters.

If your request for donation came via email, there is a chance of it being a phishing attempt.
Do not click on the link in the email and volunteer your bank account or credit card information.

Your best bet is to contact the recognized charitable organization directly by phone or their website.

go to Contents

08 Offer of Winning a Cruise etc

These scams are most active during the summer months. You receive an email with the offer to get amazingly low fares to some exotic destination but you must book it today or the offer expires that evening. If you call, you'll find out the travel is free but the hotel rates are highly overpriced.

Some can offer you rock-bottom prices but hide certain high fees until you "sign on the dotted line". Others, in order to give you the "free" something, will make you sit through a timeshare pitch at the destination.

Still others can just take your money and deliver nothing.

Also, getting your refund, should you decide to cancel, is usually a lost cause, often called a nightmare or mission-impossible.

Your best strategy is to book your trip in person, through a reputable travel agency or proven legitimate online service like Travelocity or Expedia.

go to Contents

09 Make Money Fast – chain mails

A classic pyramid scheme: you get an email with a list of names, you are asked to send 5 dollars (or so) by mail to the person whose name is at the top of the list, add your own name to the bottom, and forward the updated list to a number of other people.

The author of this scam letter painstakingly explains that, if more and more people join this chain, when it's your turn to receive the money, you might even become a millionaire!

Bear in mind that, most times, the list of names is manipulated to keep the top name (the creator of the scam, or his friends) on top, permanently.

As with the previously circulating snail-mail version of this chain, the email edition is just as illegal. Should you choose to participate, you risk being charged with fraud – definitely not something you want on your record, or resume.

go to Contents

10 Turn Your Computer Into a Money-Making Machine

Although not a full blown scam, this scheme works as follows: You send someone money for instructions on where to go and what to download and install on your computer to turn it into a money-making machine… for spammers.

At sign-up, you get a unique ID and you have to give them your PayPal account information for the "big money" deposits you'll "soon" be receiving. The program that you are supposed to run, sometimes 24/7, opens multiple ad windows, repeatedly, thus generating per-click revenue for spammers.

In other scenario, your ID is limited to a certain number of pages clicks per day. In order to make any money whatsoever from this scheme, you are pretty much forced to scam the spammers by hiding your real IP address with Internet proxy services such as "findnot", so you can make more page clicks.

We will not go into the discussion about what this program will do to your computer's performance... it is a true tragedy if you get conned into this scam. You will then have to call a computer expert.

go to Contents

11 Tax and TV Refund

First and fore most neither Inland Revenue nor TV companies will email you. That is the first sign. If in doubt delete it.

12 Phone Calls

When you receive a phone call stating that it is from the police, tax men, lawyer, bailiff or any one, be calm. Do not divulge any information about you. Get all the information about them: Name,

person's ID Number, company name, address and phone. Then put the phone down. If they call back let them know that you have emailed their information to the Crime Branch.

go to Contents

E-Mails That are Scam

Some emails will look as if they are from your contact list.

E-Mail from familiar person, Never click on the Link

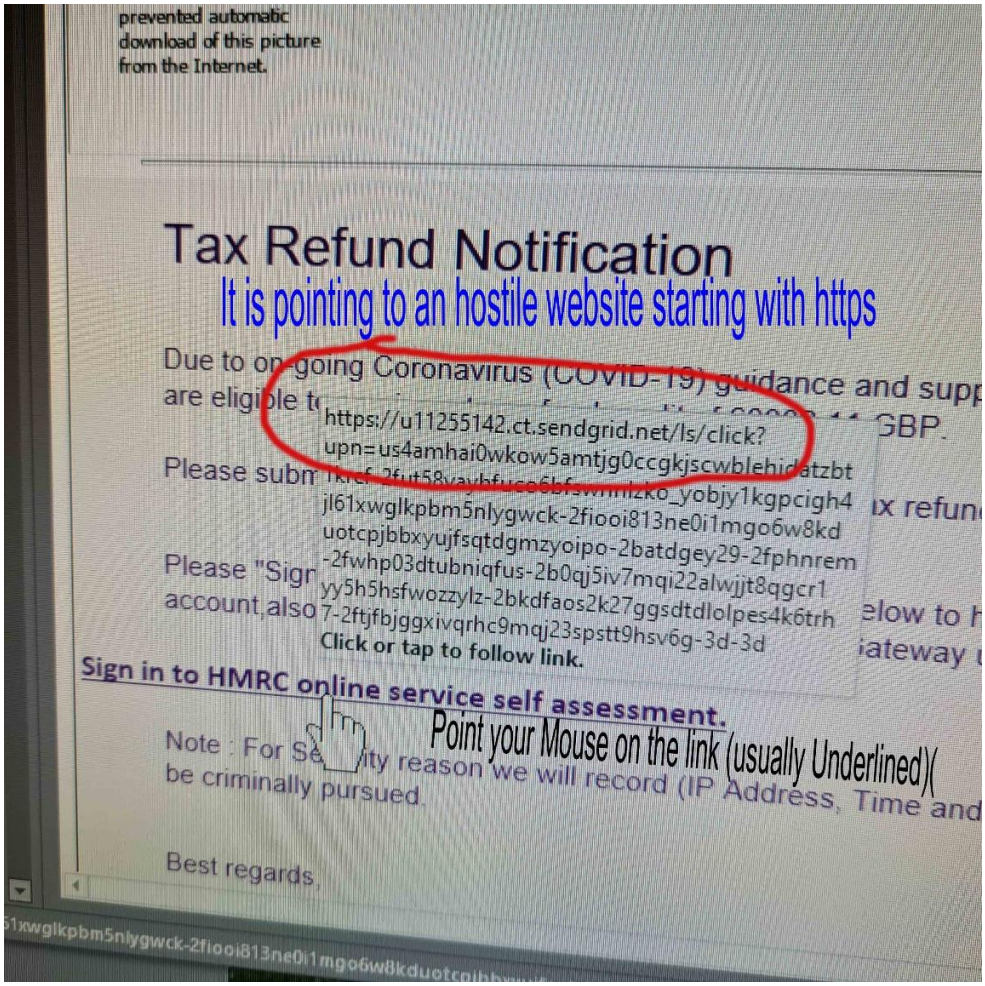

Figure an HMRC Scams - pointing to a hostile website

go to Contents

 Thank you to askleo.com for the information