Acuris Risk Intelligence

# Acuris Risk Intelligence

# CyberCheck:

## Frequently Asked Questions

Acuris Risk Intelligence

Acuris Risk Intelligence

## Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 25/09/2019 | 1.0 | Document Creation | Matt Taylor |
| 11/02/2020 | 1.1 | New Content Added | Matt Taylor |
| | | | |

Acuris Risk Intelligence

# Contents

## Points to remember

- Once data appears on the dark/deep web, there is no way of removing it or getting that data back.
- Criminals will not hold your data for any legitimate reason, if they have it you are at risk.
- We do not add, alter or amend any of the data found. Knowing exactly what data the criminals hold about you empowers you to take positive action to reduce the risk of you or your family becoming a victim of ID fraud.
- In the vast majority of cases you will never be made aware that your personal or financial details have been used to commit Identity Fraud. It is often not in the interest of the organisation which is the target of the fraud to notify you that a criminal has used your identity whether the fraud has been successful or not.
- You can create the strongest password possible, but it is still just as vulnerable as the weakest password if the website you have used it on is compromised.
- It is combinations of your personal data that expose you to varying levels of risk of Identity theft.

Acuris Risk Intelligence

# Research Information

## Where does the data come from?

All of the data within the Acuris Cybercheck database has been in criminal hands and made available on the internet in criminal forums, chatrooms and marketplaces. These sites are one-stop shops for criminals to buy, sell, trade or copy personal data to be used in a plethora of frauds including phishing and cold call scams.

## How did the data get there?

When people browse the internet and join websites by creating accounts or sign up to online services, they are often required to provide some information such as their contact details, some identification details and, where services are sold, financial details. While the website that initially gathers the information may do so for legitimate purposes, the site may be compromised by external agents (hackers) or by employees. Many websites are set up purely to harvest personal data for sale on the dark web. They purport to be legitimate Payday loan, Credit checking or Accident Claims websites where you would normally expect to enter more personal details than on a usual retail website. Where possible, our analysts take care to note both where the data was originally captured and where it was found.

## Data Accuracy: I don't recognise some of the data in my record – why is this? /Why is some of my data incorrect?

If some of your data is incorrect this could be for one of these reasons:

- A criminal has created additional data to enhance the information they have about you in order to get a higher price from selling it.

- You may have deliberately entered false information on a particular website you have visited that has subsequently been hacked.
- Law enforcement or Anti-Fraud Organisations have identified personal/financial data being made available for fraud and deliberately amended the data in such a manner that it will disrupt any future criminal activity.

# Risk Analysis

## Overall

Obviously, the more information the scammers have about you the more attractive you are to them. That 'one' further piece of personal information they hold about you is pivotal in their decisions as to whether to target you or not. If fraudsters have your:

- Date of birth - by basic research utilising your personal details together with your date of birth they will be able to find the answers to most of the personal questions that you are likely to be asked by any financial institution such as mother's maiden name etc.
- Email address and password - They can take advantage of the fact that many people use the same password/secret answer for the websites that they use which require registration. Together with your email address, which very often is your 'Username', the scammers have plenty of incentive to surf various websites, where you may be a member.
- Social Security Number - Not as important outside of the USA and Canada but the possession of an SSN together with associated personal data makes it very easy with minimal additional research to compromise a victim’s identity.

## Low Risk

### Email Address Only

Vast lists of email addresses are circulated on the World Wide Web and are used for marketing (spamming) campaigns usually for insalubrious products. We ignore these lists but do copy email only lists if we find them posted in a criminal forum for a specific purpose such as a phishing fraud with emails pretending to originate from a Bank or Government Agency. These lists tend to be much smaller in an attempt to bypass the anti-spam software employed by most email providers.

Despite only knowing the email address about the addressee these phishing emails are surprisingly successful in extracting personal data from victims as they use copy templates of the legitimate banks/Government own websites and logos.

In this day and age no Bank or Government Agency will email you directly seeking personal/financial information. If we have just your email in the Cybercheck database be conscious when receiving any email requesting such information.

## Low – Medium Risk

If the criminal has a name or partial address together with an email address for an intended victim, they will be able to personalise the phishing email which increases the chance of a successful phish.

## Medium Risk

### Name + Address + Landline phone number (UK)

Where can people find these details now that telephone directories are no longer commonplace? Criminals will not pay to use 192 or 118118 as they are expensive. They purchase large lists of data which have either been hacked or originates from marketing lists that have ended up in criminal hands. These lists are used for cold calling and to commit pension, investment or account takeover frauds particularly as it is more likely that you will answer a landline call rather than a mobile call from a number you do not recognise.

The usual advice to be aware that if you receive calls from anyone offering something that is too good to be true that's because it is, still stands good. However, criminals have developed sophisticated cold calling techniques that are purely designed to extract personal, financial or security data from innocent victims to be used at some later stage in frauds that could not be connected back to the call.

If you receive a phone call from someone purporting to be from your bank/building society or Government Agency seeking personal or financial data do not pass over any such details. Ask for their name, department and phone number and tell them you will ring them back. Look up the department they say they were from on the internet and check to see if the phone number matches. Only then if you are totally satisfied the call was legitimate call them back. If you are in the slightest doubt do not call them back, if it was legitimate, they will find another way to correspond with you.

## Medium – High Risk

### Name + Address + Mobile phone number

Where could a criminal find your name, address and mobile number in one place? Criminals obtain this information from databases that have been compromised where in the past you have completed these details, for example a mobile phone provider or where you have made a purchase online which required you to provide a mobile number. What increases the risk of successful cold calling/phishing is that the criminals have the technology to display the legitimate telephone number of the institution they are pretending to be from on the victims' mobile screen.

As with landlines, the usual advice to be aware that if you receive calls from anyone offering something that is too good to be true that's because it is, still stands good. However, criminals have developed sophisticated cold calling/phishing techniques that are purely designed to extract personal, financial or security data from innocent victims to be used at some later stage in frauds that could not be connected back to the call.

If you receive a mobile call from someone purporting to be from your bank/building society or Government Agency seeking personal or financial data do not pass over any such details. Ask for their name, department and phone number and tell them you will ring them back. Look up the department they say they were from on the internet and check to see if the phone number matches. Only then if you are totally satisfied the call was legitimate call them back. If you are in the slightest doubt do not call them back, if it was legitimate, they will find another way to correspond with you.

## High Risk

### Email + Password

Email addresses are becoming synonymous with usernames, and most websites that you have to register on use the email address as your user name. Human nature dictates that we will often use the same password on different websites, and this is what criminals rely on. If a criminal has obtained your email and password from such a website, they will used software called “Checkers” that will target other websites that the criminal believes you may have visited and used the same password. If they are successful, they will be able to

- To alter, add or copy any of your other personal details you have included when you registered with the website.
- To obtain any financial details you have registered and saved on that website.

By taking note of the nature of the website with which you have registered, they may visit similar sites to see if you have registered with them using the same password. The criminal will try social networking sites using the email and password and this not only opens up further aspects of your life but also details of your friends.

A worse scenario occurs when the criminal, knowing your email domain, can gain access to your emails. Not only are all your personal communications exposed but a criminal now has the ability to deliver viruses and trojans to your network of friends or work colleagues from your email address, which they will automatically trust, as you are the sender.

**Important** – If you believe that your email/password may have been compromised you should check the “Message forwarding” section of your email provider to ensure a criminal has not arranged for all your emails to be forwarded to them.

## Passwords

I no longer use that password, but you keep notifying me it has been posted on a criminal website?

Is that really true – have you changed that password on every single site where you may have used that password in the past?

Once a criminal has no further use or interest in any data, they frequently post that data on open source forums to be used by other lower level criminals and effectively cover their trail. This data will be copied and posted in different forums which is where we have identified it.

Whenever we notify you that your data has been found it would be worth taking a minute just to consider if you have changed that password on every website you may have used it on.

## Credit Card details

You have found my card details are compromised, why has my card issuer not contacted me?

A credit or debit card is costly to replace as well as take up staff time in contacting you which they will try to avoid. They may deal with information in different ways, such as:

- The card issuer may not have been aware your credit card has been compromised.
- Many card details that are stolen are never used and the issuer may decide to monitor the usage on the card and only cancel the card if any unusual activity takes place.
- If the card is due for renewal in the near future, they may issue the new card earlier
- If the card has expired, this could be because it was part of a batch of cards that were traded that included both current and expired cards – the criminals buying the batch expect that not all the cards will be current and that will be reflected in the price they pay.
- If we have your card details (especially if it has been traded after the card has expired) you should look at the personal data that has been found alongside the card as this will be the data the criminals will be looking to exploit and take the necessary precautions as advised.

**Important –** If we have found your credit card details (current or expired) and you have not been informed that your card was compromised by your card issuer, you should contact them to ask whether they had knowledge of the compromise and if they were what other of your data was compromised that they were aware of?

**Note** - In the past 10 years we have passed the details of over 1,500,000 stolen credit cards to Law Enforcement Authorities or directly to the issuing banks. If you were notified in the past that your card was compromised it may have been because of our intervention.

## Bank Account details (UK)

You have found my bank account details, what risk does this pose to me?

Details of bank accounts together with personal data are used as "Proof of funds" to set up lines of Credit or for Direct Debits, Standing Orders etc necessary to pass Credit checks for servicing ongoing monthly contracts such as mobile phones, car payments etc.

They are used to attempt to transfer any available funds out from those accounts or associated accounts operated under the same name such as ISA or deposit accounts.

If the criminals have a level of control over the account, they may use it to launder monies obtained from other successful frauds. Accounts use in this way are commonly known as "Mule" accounts and it can be very difficult to prove that you had no knowledge your account was being used in this manner.

**Important –** If we have found your bank account details and you have not been informed by your bank, you should contact them to ask whether they had knowledge of the compromise and if they were what other of your data was compromised that they were aware of? If they were not aware you should notify them of the details, we have found and ask for your account to be monitored by them for unusual activity in the future.

## National Insurance, Driver Licence details Passport details (UK)

Any additional information the criminals have about a victim increases the likelihood of them being able to commit a successful fraud and also opens up the variety of frauds available for them to commit. For example, using a victims drivers licence and National Insurance number details have enabled criminals to apply for taxi drivers positions online on behalf of persons not entitled to work who then assume the victim's identity and take up the role.

## Incorrect Bank, National Insurance, Driver Licence details Passport details (UK)

The Bank account/ National Insurance/Drivers Licence/Passport details you have associated with my personal details are not mine - why?

There are three basic explanations: -

When criminals are seeking Loans, Credit or obtain goods or services which require a Direct Debit/Standing order to be set up such as mobile phones they create sort codes and account numbers that match the algorithms used by the banks. They may do the same with National Insurance, Driving Licence and Passport algorithms. These accounts etc do not exist but are sufficiently accurate to satisfy the organisations checking requirements when combined with the use your personal data.

The criminals may have enhanced your real basic personal data with false financial/Driving Licence etc details in order to increase the price they are able to sell or trade it on for to other criminals. Do not believe there is "Honour among thieves"!!

When personal and financial data is hacked from organisations it is usually in a structured format like a spreadsheet. The criminals dissect and post this data in the same spreadsheet format. This enables Law Enforcement and other Anti-Fraud organisations to subtlety alter the data as simply as moving part of line down in a spreadsheet. This means your correct personal data is then matched with the correct financial/DL data etc of somebody else. If used together in attempt to commit a fraud they will invariably fail on most occasions and the disruption has been successful.

**Important** - If you have not been aware of an Identity Fraud using your correct details together with other false data, ensure you check your credit report in case the false data has been associated with your credit report filing

## Date of birth

The date of birth you hold for me is incorrect:

There is no mileage in the fraudsters inventing a date of birth for you. That leaves the following possible explanations:

1. We have identified what we believe to be your date of birth from amongst the information that has been circulated about you. There is the possibility that the date shown is actually the answer to the secret question 'What is a memorable date to you?'

2. You have been suspicious about the phishing email or website to which you have given your personal details and have given an incorrect date of birth. If all your other details that we hold are correct, this is the most likely scenario.

3. The date is part of a Captcha/I am not a Robot process which we have wrongly identified as your DOB.

4. Someone else's DOB has been appended to your record after intervention and amendment by Law Enforcement/Anti-Fraud Organisation (see incorrect bank details)

## Secret Answer

I do not recognise the Secret Answer associated with my record.

- There are several possible reasons for this.

- The secret answer has been created by a criminal in your name
- We have incorrectly identified data we believe is a response you have given to a “Secret Question”
- Someone else’s secret answer has been appended to your record after intervention and amendment by Law Enforcement/Anti-Fraud Organisation (see incorrect bank details)

### Employer

To commit “Director Fraud” criminals require the details of company staff members together with the readily available Company Director details. If your name appears together with your company email address and company mailing address be aware if you receive email requests from Senior company staff members to make urgent payments to alleged creditors.

Acuris Risk Intelligence

## General Advice

For UK clients - There are a number of places you can go to receive advice and guidance on how to protect yourself. The UK government supports several websites, for example see:

- Take 5 to stop fraud (https://takefive-stopfraud.org.uk/)
- Cyberaware (www.cyberaware.gov.uk)

In general, you should check your credit report regularly for any activity that you did not do yourself be they applications for credit or changes to personal details.

Use a reputable anti-virus software to protect your PC, laptop or other devices.

If you do find that any of your personal information has been compromised there are a number of things you should consider doing:

Contact your bank or credit card company and tell them you wish to have either additional secret questions to the usual mother's maiden name or date of birth, or to replace them entirely. Do not pick a question like 'what is your favourite team' as they are easy to guess. Be abstract, but it must be memorable – for example, 'what is the subject of the picture on my front room wall?'

Use 'disposable' passwords for websites you need to register on and don't use the same one elsewhere. If you need to visit the website again, once you have entered your username / email address they invariably have a 'forgotten your password' facility which will then send a new password to your email address when clicked.

Acuris Risk Intelligence

# General FAQs

## My details appear multiple times and the source and date are the same for each entry?

This has occurred when criminals have merged previously hacked email/password lists into one larger one commonly referred to as a "Combolist" or "Collection". These can consist of 100's /1000's of different hacked email/password lists and can contain in excess of a billion entries. Your details will have been in different hacked email/password lists which once merged produce multiple results within the one larger dataset.

## My Telephone/Mobile number or Email is linked to another person's details?

We have reproduced the data as it was posted.

If you have been the victim of an attempted identity fraud or an actual identity fraud, these may be the details that were used by the fraudster

Your details may have changed as a result of "Disruption" tactics by Anti-Fraud Organisations (see Incorrect Bank details)

Your details may have been added to other data by criminals in order to enhance its perceived value.

**Important** – Your mobile/landline/ email may have acquired its own "Digital Identity" associated with the incorrect details. Whilst nothing can be done with such data on the Dark Web it may well have leaked onto the World Wide Web.

Search your email address and phone numbers in the Google browser ensuring they are contained with speech marks. i.e "johnsmith123@hotmail.com" / "7234567890" etc. This should indicate if they have found their way onto the Worldwide web and are now open source.

## Only a partial portion of my password is shown in the database, do I still need to change it?

Yes, when trading stolen email credentials criminals will often encrypt, obscure or remove characters to disguise the real details, which will be revealed once they purchased.

## What are "VoucherValue/VoucherValue1"?

These are our random fields and contain data that should be recognisable to you as the subject of the record. For example, these fields may contain information concerning Loyalty schemes, Mobile Phone contracts or Utility accounts, basically any data that was found together with your other details that we believe may help you identify the source from where your data originated"

## I have been informed an Organisation/Website where I have registered has been hacked, will my information be available in your database?"

Not all data that has been obtained following data breach will ever find its way onto the dark web, if that is the case, we will not have your data in our database. However just because a database where your data is stored has been breached does not necessarily mean your data has been compromised. Complying with legal regulations in many countries or just company policy means that the hosting organisation may report the "Worst case" scenario meaning the very maximum amount of data that could have been exposed is reported

not what actually may have been compromised. Responsible companies will inform you if your data was part of the compromised data.

Whether or not your data was exposed, take the opportunity to spring clean all your passwords and check your credit report regularly.