Voice Call, Email Phishing and SMS Text Fraud Attempts Surging....

We have been seeing a significant increase in calls to us from victims/attempted victims of these types of identity theft and fraud.

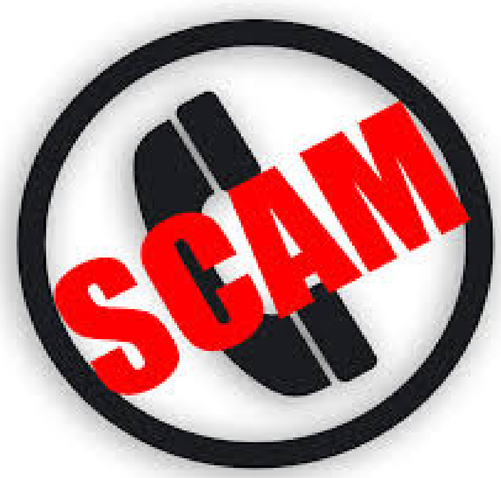
So we thought we'd provide some repeated guidance on what to look out for and some DO's and DONT's

Identity Fraudsters are becoming increasingly sophisticated in their use of the latest technology to try and con us into believing they are a "legitimate" representative of a company.

The quality of the fraudulent emails/texts/and voice calls is such that unless we are very vigilant we can be duped.

Typical ploys include:

- Calling to inform you that your account is overdue and demanding payment
- Advising you that your account has been compromised and asking you to allow PIN Code and Password Resets
- Asking you to confirm suspicious activity on your account and allowing them access to investigate further
- Calling to "confirm" recent purchases on your account
- Text messages from a "friend" eminating from a number you don't recognize
- Informing you that you have been part of a data breach and you need to supply them with personal information to help "protect you"
- Emails that look like they are legitimate (logo, content etc) asking you to "click on a link" to obtain information or a "free gift"
- Calls saying that a purchase was inadvertently charged to your account and they need your information to cancel the transaction.



DO	DON'T
Verify the number that is calling you is a vaild phone number for the company calling. If in the slightest doubt, HANG UP and check. Ask for the name and ID# of the representative.	Give out ANY personal information unless you are absolutely sure it is necessary and being given to a vaild representative. Don't assume that just because the voice "sounds" like a friend or co-worker that it is them, especially if it's an unusual request or conversation.
Change PIN Codes and Passwords regularly and where avilable enable 2 Factor Authentication (2FA).	Give out PIN Codes or Passwords or allow them to be changed by a third party. If a caller/texter/emailer asks for this, go to the company website and see if you can do it there or call back the company and ask why it's necessary.
Ensure your computer/mobile device software is up to date and has the latest security "patches" installed. Ensure that you have your "spam" and security filters set up correctly.	Open emails that look suspicious or click on links from a non verified source. You may be importing malware and data "scraping" software.
Ensure you think about what's on your social media profile and who has access to it. Social Media is a treasure trove for scammers.	Allow people to "follow" or "friend" you unless you know them and you are happy for them to be in your social media circle. Never give out personal information over social media platforms unless to a verified source.
When in doubt, check phone numbers on official websites and on the back of credit cards etc. Use these and ONLY these to return calls or verify enquiries	Call back to a number given by a suspicious caller purporting to be from a bank/credit card/government agency. Hang up, and check.

When all is said and done, WE are the first line of our defence against fraud. We need to be vigilant, use common sense and be extremely cautious with our information. When in doubt DON'T

More Information? Call Us... 877 308 9169

www.idresolution.net