



# **Digital Fraud**

## **How Can I Protect Myself? – What Do I Do if I'm a Victim?**

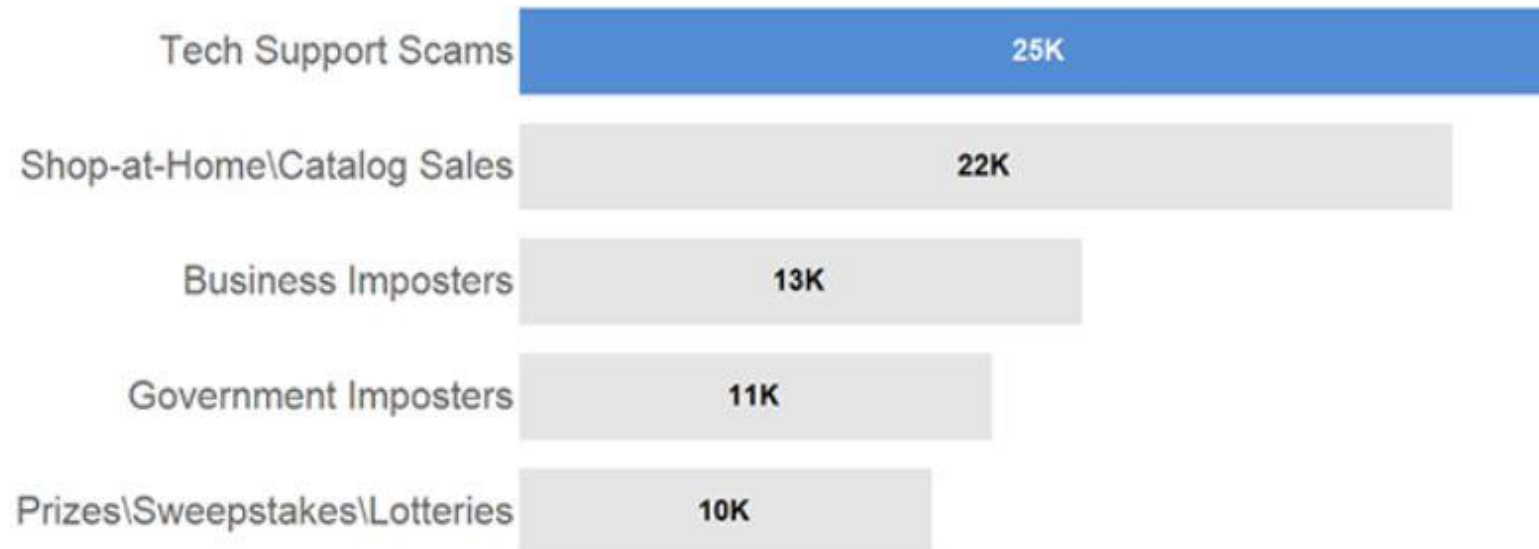
---

---

# How Do Scams Happen – General Attack?

## Ages 60+ Top 5 Fraud Categories by Number of Reports Indicating a Loss

Older adults filed more reports indicating a loss on tech support scams from 2015 to 2018 than on any other Sentinel fraud category



## Avoid this genetic testing scam

Have you heard about the latest scam? Scammers are offering “free” genetic tests and claiming Medicare will cover it — so they can get your Medicare Number and use it to commit fraud and identity theft. They’re targeting people through telemarketing calls, health fairs, and even knocking on doors.

**Only a doctor you know and trust should order and approve any requests for genetic testing.** If Medicare is billed for a test or screening that wasn’t medically necessary and/or wasn’t ordered by your doctor, the claim could be denied. That means you could be responsible for the entire cost of the test, which could be thousands of dollars.

[Learn More](#)

### Here’s how to protect yourself:

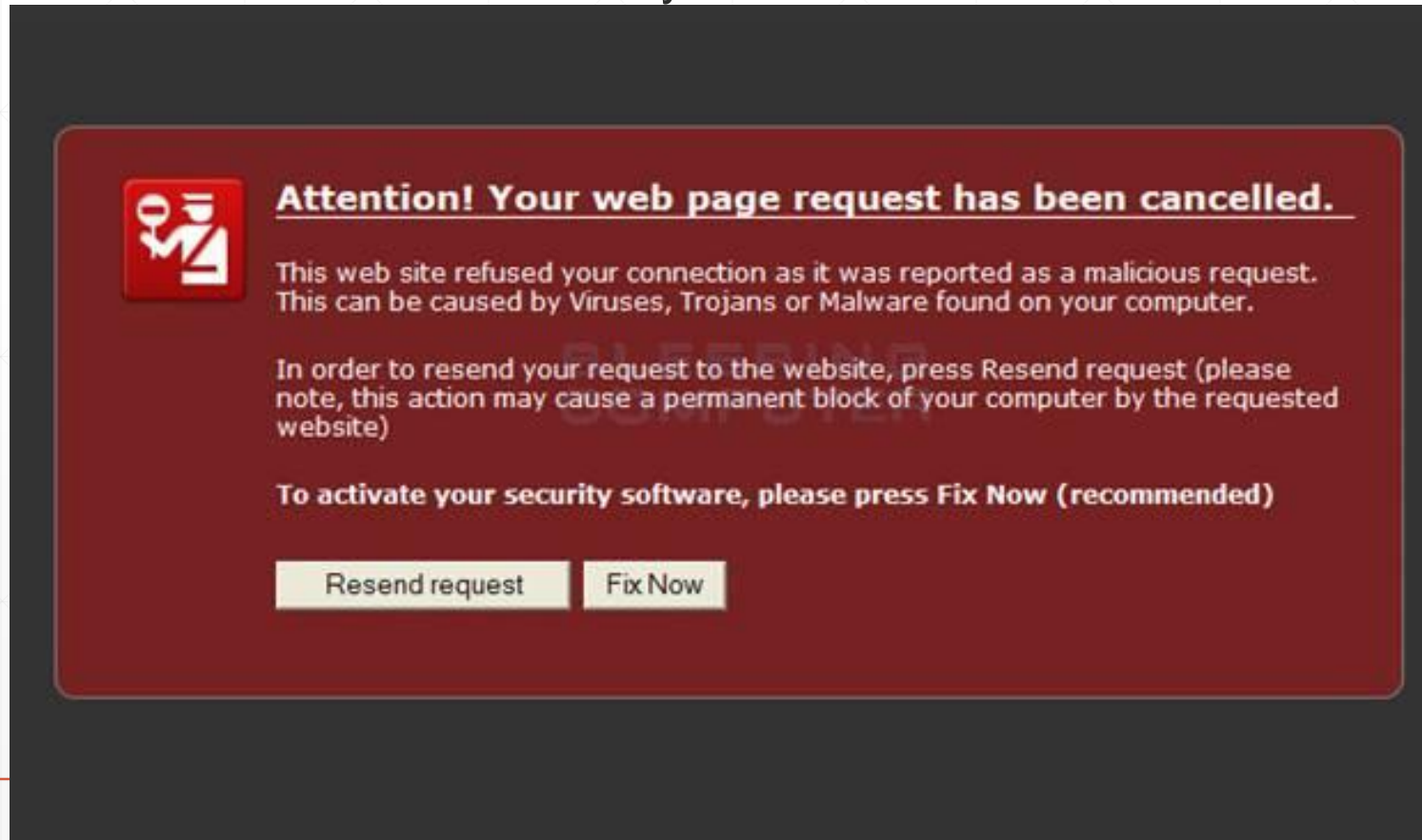
- **Don’t share your Medicare Number, Social Security Number, or other personal information** with anyone who offers to give you a “free” in-person genetic screening or cheek swab, or a DNA testing kit in the mail.
- If you get a genetic testing kit in the mail, **refuse the delivery or return to sender** unless your doctor ordered it.
- **If you suspect Medicare fraud, call 1-800-MEDICARE.**

# How Does it Happen

- Phone Call
  - Physical
    - Mail box
    - Wallet (lost or stolen)
    - Trash
  - Social Media
  - Browser Malware
  - Phishing
-

# Browser Hijacking – Resulting in Tech Support Scam

- An infected website takes over your browser



# Phone Numbers You Should NEVER Call

- Browser frozen with a terrible warning message and a number to call to recover
  1. do not call the **phone number** - Close and Reset the browser  
or
  2. Come to the Resource Center
- You Google for help on something and get a **phone number** to call for support
  - Yikes! Don't call it unless you are **absolutely, positively, 100%** certain it is a real support group. Even then, when they ask to take control of your PC, hang up and come to the club!

To Get Support from a technology company, go to their website and follow the Support tab

- [www.thetechcompany.com/support](http://www.thetechcompany.com/support)
-

# Spoofting Email

**From:** Officail 365 Message Center <[alerts@newoffice.com](mailto:alerts@newoffice.com)>  
**Sent:** Thursday, June 21, 2018 12:21 PM  
**To:** [Redacted]  
**Subject:** Help Secure Your Account

**Please Sign in again.**



Dear [Redacted],  
Please sign in to re-confirm [\[Redacted\]](#) ownership.

**Confirm ownership**

Best Regards,  
**Note:** *We will never ask you for your payment information just account password confirmation.*  
2018 © Microsoft Data.

Look for something.com/..... when you hover over the link

# How Does it Happen?

## Data Breaches in 2018

Company	Breached	Content
Aadhar	1.1 Billion	Names, ID number, bank accounts, etc.
Marriott Starwood Hotels	500 Million	Phone, email, passport #, CC #
Exactis	340 Million	Phone, address, personal interests, character
MyFitnessPal	150 Million	Usernames, email addresses, passwords
Quora	100 Million	Names, email addresses, passwords, linked info
MyHeritage	92 Million	Email addresses, passwords

### Plus

State of SC Income Tax Records (2012 – everyone since 1998)

Credit Card from retailers

---



# Preventing Identity Theft –Digital Actions

- Remember that every online service you have has a sign in requirement
    - **Username** which is your email address
    - **Password** which you select yourself
  - Since you can be pretty sure that one of your accounts has been included in a major breach, **Why would you use the same password on multiple accounts?**  
[HaveIBeenPwned.com](https://HaveIBeenPwned.com)
    - You **MUST** use an organized way to remember passwords – manual or automated or system like Last Pass
  - Critically important accounts should have two step authorization activated
    - Financial and email and ...?
  - Consider Purchasing Identity Theft Insurance
-

## **Preventing Identity Theft – Physical Actions**

- **Set up Alerts in your financial accounts**
  - **Do not mail checks or other payments in an unprotected mail box**
  - **Be aware of the cards in your wallet – have a plan for losing your wallet**
  - **Be aware of the information you have in your house – a break-in could cost more than a TV**
  - **File Income Taxes early**
-

# How Do I Know If It Has Happened To Me

- Balance Your Bank Account
  - Verify Your Credit Card Purchases
  - Review Your Credit Report Quarterly
    - Loans or accounts you don't know about
    - Drop in credit score for unknown reason
  - Take Immediate Action IF
    - Your mail is held or forwarded
    - You receive a statement or bill from an organization you don't do business with
    - Other indicators of financial activity you didn't initiate
-

## What Do I Do If It Happens To Me



- [www.identityTheft.gov](http://www.identityTheft.gov)
    - Social Security Administration automatically notified
  - File a Police Report
  - Contact Your ID Protector
  - Develop a Recovery Plan
-

# Password Management Systems

- Systems that do it for you
    - Last Pass <https://www.lastpass.com/>
    - DashLane <https://www.dashlane.com>
    - Keepass <https://keepass.info/>
    - 1Password <https://1password.com/>
    - RoboForm <https://www.roboform.com/>
  - Your own Word document or Spread Sheet – Encrypt it!
  - A note book - not a “diary” with instructions in it
    - Username which is nearly always an email address and your password for that business
  - Last Pass Class on November 14
-

# Two Step Verification

- Best protection for accounts with money associated with them is “**Two Step Verification**”
    - Provided by the Company you are dealing with
      - Vanguard
      - Microsoft
      - Apple
      - Google
      - Etc.
  - Step one = username and password
  - Step two = texted code on your cell phone
-

# Identity Theft Protection Services

1. ID Shield ([www.idshield.com](http://www.idshield.com))
  2. Identity Guard ([www.identityguard.com](http://www.identityguard.com))
  3. Trusted ID ([www.trustedid.com](http://www.trustedid.com))
  4. Lifelock ([www.lifelock.com](http://www.lifelock.com))
  5. All Clear ID ([www.allclearid.com](http://www.allclearid.com))
  6. ID Watchdog ([www.idwatchdog.com](http://www.idwatchdog.com))
  7. FreeCreditReport.com
-