

Hilton Head Island Computer Club



Members Helping Members Learn Technology Since 1989

The Basics of Digital Security

March 25, 2024

CONSUMER
SENTINEL
NETWORK
DATA BOOK 2023



SNAPSHOT

5.4
MILLION
REPORTS

TOP THREE CATEGORIES

- 1 Identity Theft
- 2 Imposter Scams
- 3 Credit Bureaus, Info Furnishers and Report Users

2.6 million fraud reports

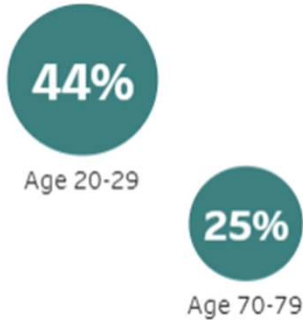
27% reported a loss



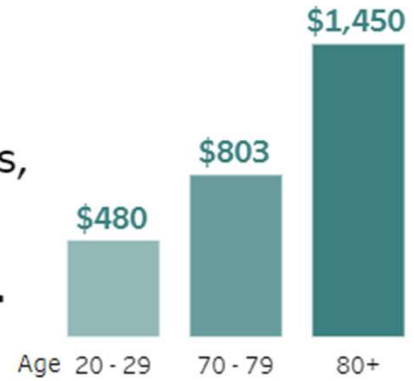
\$10.0 billion
total fraud losses

\$500
median loss

Younger people reported losing money to fraud **more often than older people.**



But when people aged 70+ had a loss, the median loss was much higher.



Imposter Scams



ABOUT
1 in 5
PEOPLE
LOST MONEY

\$2.668 billion
reported lost

\$800 median loss

Identity Theft Reports

82% ↑

Government
Benefits Applied
For/Received

51% ↓

Medical Services

FEDERAL TRADE COMMISSION • ftc.gov/data

Data as of December 31, 2023

1. Identity Theft

- **Usually done by individuals or small groups – “local thieves”**
- **Obtain Information**
 - Information : Social Security Number, Birth Date, Bank Account, Physical Address
 - Online data breaches
 - Physical theft (out of your mailbox, from your phone, from your wallet)
- **Use Information**
 - Open accounts, obtain medical services, obtain loans
- **Protection**
 - Monitor your accounts and your credit ratings
 - Identity Theft Insurance

2. Imposter Scams

- **Imposter Scammers Are Everywhere (trying to earn a living!)**
 - Phone Calls
 - Emails
 - Texts
 - Social Media (Facebook, TikTok, etc.)
- **They are trying to get information about you that they can sell**
 - Credit Card info
 - Bank Account info
 - Social Security and Birth Date
 - Website Sign In Information (Amazon, eBay, Walmart, ...)
- **Or they are trying to get you to send them money**
 - Romance scam
 - Grandkid scam

Who are “they”

- Individuals trying to earn a living by selling or using personal information from the dark web. (credit card info about \$17)
- Small groups trying to do Identity Theft by gaining your personal information and opening accounts or making purchases in your name
- Organizations trying to get you to send them money through personal contact (tech support scam, romance scam, investment scam)

Individuals in any place where there is internet service

Groups in poorer countries with strong tech training: Philippines, India, Nigeria, Malaysia, etc.....

Credit Card Theft – The Process

Stolen Credit Card Numbers: The Endgame (Forbes December 2023)

Steps of a hypothetical credit card heist:

1. Credit card details, up to and including a cardholder's SSN, are stolen in a data breach. (example – MGM resorts in September, 2023)
2. The criminals responsible collect all of the information they've acquired, including tens, hundreds or thousands of cardholders' individualized data, and put it up for sale on a dark web marketplace.
3. The list is bought by another group and possibly quality tested for legitimacy. The stolen data stays in circulation anywhere from minutes to days to years.
4. Someone buys and begins to use the stolen data to make purchases either online or in physical stores using fake cards. They resell these purchases for cash.
5. Hopefully, this causes individual consumers to receive a notification about suspicious activity from their bank(s). Before the situation can worsen, these consumers are able to cancel their cards and successfully contest the purchases.

While this is overly simplified, it highlights the journey credit card details make once they are stolen.

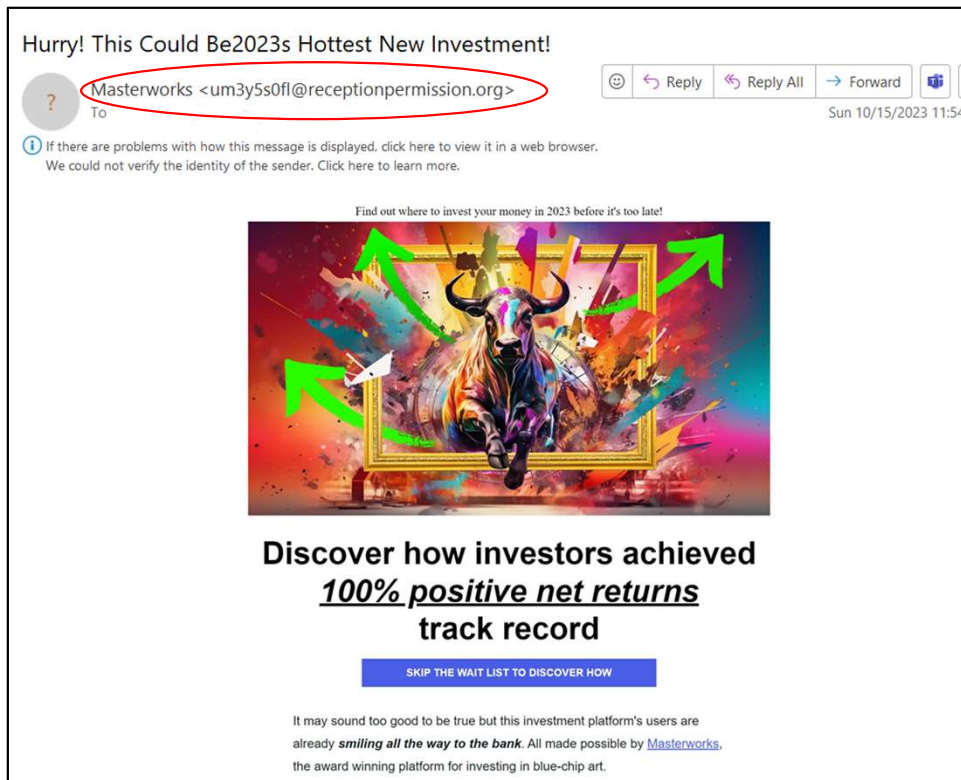
What HHICC sees the most:

Scam –
Phishing Emails
and Texts

Hijacked
Browsers

Fake Tech
Support

Scam – Phishing Emails



Check the senders Domain
@XXXXX.XXX

If it's not a *company.com*, spelled correctly, do not trust it

If you don't trust it, DO NOT
Unsubscribe!!!

Move the email to your junk folder

Norman Galloway

From: Peacock Membership <Drint.Aznu247@sheridancollege.edu.pl>
Sent: Tuesday, October 31, 2023 5:47 PM
To: [REDACTED]
Subject: RE:Extend your account for free !



Your Membership
has expired!



Dear customer,
Your Peacock Membership has expired

But, as part of our loyalty program,
you can now extend for 90 days for
free.

Extend for Free

* After signing up, you have to insert your credit
card details for validation of your account
We **will not** withdraw any amount.

Norman Galloway

From: Holiday Money <cp6vzw@consensusmarkterrify.co.uk>
Sent: Friday, November 3, 2023 12:37 AM
To: [REDACTED]
Subject: Happy Holidays! Redeem YourCash Offer

**GET UP TO \$2
IN 3 EASY S**

 EASY LOAN REQUEST

 FAST LOAN PROCESS

GET S

* See site for details.
This offer may not be valid in Arkansas or
To stop receiving messages, [visit here](#) c

Scam Phishing Text Messages



+44 7754 337343












+44 7754 337343



+44 7754 337343

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link. <https://u-sps.co>


USPS - Linkfly

←   <https://u-sps.co>         

Microsoft Edge Would you like to set Microsoft Edge as your default browser? [Set as default](#) [Not N](#)

USPS

Your package is on hold for an invalid recipient address. Fill in the correct address info by the link.

	Click Update
	Privacy Policy
	Terms of Use

Text Scams

If you don't recognize the phone number, don't click on any links and don't call the number or reply.

Types of Text Scams

- **Copycat bank fraud** – “call immediately, we've seen a suspicious transaction in your checking account”
- **Bogus gift scam** – you've been selected to receive an iPhone 17
- **Friend scam** – “stick the pig” : developed over weeks or months, financial opportunity
- **Grand child emergency**

Hijacked Browser - We see this a lot!!!

- You go to a website and all of a sudden, your screen is locked with some big warning message and a phone number to call for help! **Don't call the number!**
- Do not click anywhere in the browser screen.
- Hold the power button down for 15 seconds – “hard stop”
- Reboot – when you first open your browser, Do NOT “reset”



Fake Tech Support

- Warning message on a website with a phone number to call
- Pop-Up message or notification
- Unsolicited phone call offering help
- Searching the web for a phone number to call for tech help (real tech companies won't list their phone number in a web search)
- **In every case, just say no!**
 - Do not let anyone take over your computer unless you know certainly that they are a “trusted provider”
 - Do not purchase an annual contract.

Some Simple Online Safety Rules

- Do not use a password more than once – any account you have may be subject to a data breach! (MGM breach last fall!)
- When you chose a password, do it uniquely – changing a single letter or symbol makes it easy to remember, but they are “cracked” by machines that are good at guessing and will start with one they know you used.
- Have a way to store and retrieve all of the username and passwords for all of your different accounts.
 - 1. Password Manager, 2. Document stored in the cloud (iCloud, Google Cloud, OneDrive) – should be encrypted, or 3. Written in a notebook or password book not stored on your physical desktop.

Identity Theft Insurance

US News 2023 list

- [**#1 IdentityForce** – Best Identity Theft Protection Service of 2023](#)
- [**#2 IDShield** – Best for Identity Recovery Assistance](#)
- [**#3 \(tie\) Aura**](#)
- [**#3 \(tie\) Zander** – Best Budget Identity theft Protection Service](#)
- [**#5 \(tie\) Identity Guard**](#)
- [**#5 \(tie\) ID Watchdog** – Best for Customized Identity Monitoring](#)
- [**#7 \(tie\) ReliaShield**](#)
- [**#7 \(tie\) LifeLock** – Best for Computer and Device Protection](#)
- [**#9 \(tie\) IdentityIQ** – Best for Family Protection](#)
- [**#9 \(tie\) myFICO** – Best for Detailed FICO Scores](#)

ID Shield

Monitors many types of records for changes

Monitors the Dark Web for “information for sale”


Sends details on any alerts

Sends monthly status

Provides Recovery Help and Insurance

(This is not an advertisement!!! Just happens to be what the presenter uses)

From: [IDShield](#)
To: [Joe Smith](#)
Subject: Account Summary
Date: Friday, March 17, 2023 8:32:24 AM



IDT FULL PLAN

Hello Joe,

As a member of IDShield, you have protection 24 hours a day, 7 days a week.

This is a summary of any activity from the past month of monitoring your identity. To view the details for an alert, please login to your account.

Monitoring Results:

Three Bureau Credit Monitoring
Scan Results: No new alerts found.

Public Records Monitoring
Scan Results: No new alerts found.

Court Records Monitoring
Scan Results: No new alerts found.

Change of Address Monitoring
Scan Results: No new alerts found.

Internet Monitoring
Scan Results: No new alerts found.

Social Media Monitoring
Scan Results: No new alerts found.

High Risk Transaction Monitoring
Scan Results: No new alerts found.

Minor Monitoring
Scan Results: No new alerts found.

[SIGN IN TO YOUR ACCOUNT](#)

Note: If for some reason the button above does not work, please copy and paste this URL into your web browser:

A Final Example from two weeks ago!

- -----Original Message-----
From: Paula Mortalo <rooneysimthemobile@gmail.com>
Sent: Tuesday, March 12, 2024 10:29 AM
To: president@hhicc.org
Subject: Yamaha grand piano 03/12/2024

Hello,

I'm offering my late husband's Yamaha Piano to any music enthusiast. If you or someone you know might value this instrument, please don't hesitate to reach out to me.

Warm regards,
Paula

The Response to an interested person

The Yamaha Baby Grand Piano GC1 model used to be owned and played by my husband who passed away last year, the dimension is "161cm by 149cm". It was last tuned sometime last year before he passed. She's about 3 years old and in an impeccable condition.

I'm relocating to France next two weeks, and I don't think my husband will be happy if I sell this piano, so I'm hoping to give it out to someone who is a passionate lover of the instrument, and you can have it if you want it or forward my email/pictures to anyone who's interested in the instrument. I wasn't going to leave it alone in an empty house.

The Piano is currently in storage in Little Rock Arkansas with the movers I employed to move my properties from my house. I can forward you the movers' contact details to enable you to contact them. The movers can deliver anywhere. I have attached pictures of the instrument for you. However, I will not be responsible for the cost of delivering the piano to you. However, the movers' rates are reasonably affordable.

I look forward to your reply.

Paula.

HHICC Online Safety Aids



Staying Safe Online Basic Tools

Most people who get "hacked" allow it to happen through unsafe behavior. Follow these recommendations.

If you receive a text or email that looks suspicious:

1. Always check the sender phone number or email address
2. DO NOT click on a link in the message
3. DO NOT call a phone number in the message
4. Look up the correct number or web address and call or go there directly.

If you have a message pop up on your screen saying your computer is infected:

1. Microsoft, Apple or Google will not tell you you have a virus. Messages that do are scams.
2. DO NOT click or call any number or link
3. TURN OFF your computer/phone/tablet (do not just put it to sleep). Do this even if the pop up tells you not to shut down your computer.
4. Restart and it should be gone. If it is still there come in to or call the HHICC Resource Center. 843-842-4475

When browsing the web:

Make sure any site you visit shows "https" in the address bar or shows a small padlock at the beginning of the address. The "s" stands for secure.

Fake "tech support" scams will try to scare you by stressing the importance of acting immediately... RED FLAG! They will also ask you to download software (usually called AnyDesk) so they can see your screen. Do not allow anyone to take control of your computer. DO NOT pay them to "clean" your device. HANG UP!

Hilton Head Island Computer Club



Members Helping Members Learn Technology Since 1989

**Stay Connected
Stay Organized
Stay Safe**

hhicc.org

843-842-4475



Never Stop Learning

Visit the Resource Center!

If you have questions about a strange Notification, email or social media message, call or come for help. We learn while we help you and can share what the bad guys are up to!