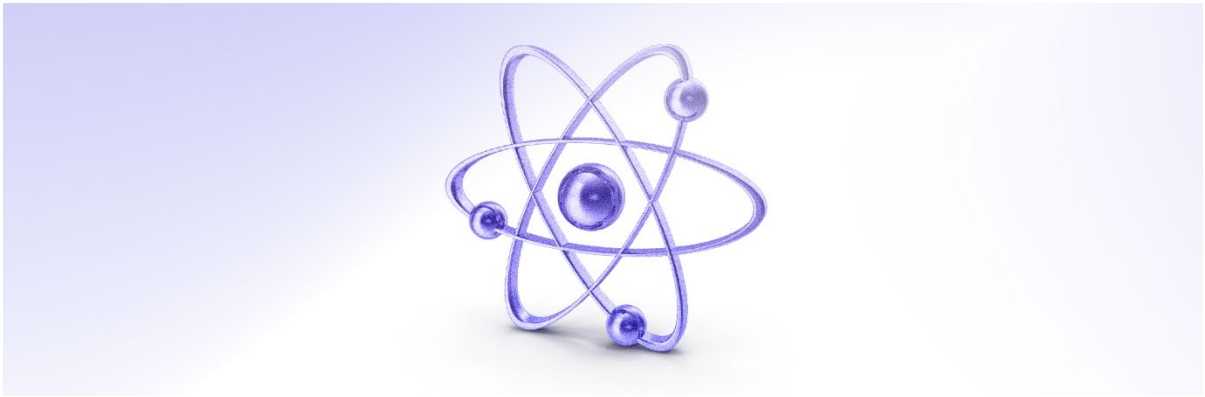
FS-ISAC | Security Tips Newsletter

17 September 2024 | Issue No. 13

Security is ***Everyone's*** Responsibility



International Fraud Awareness Week is Coming

Summary

As a consumer, you may be concerned about fraud. Perhaps you've been a victim of fraud and understand the huge inconvenience that follows as you try to undo the damage. Industries around the globe are promoting International Fraud Awareness Week during 17-23 November 2024.

The Most Common Types of Financial Scams

Visual Capitalist says, "In 2023, there were $485.6 billion lost in total from financial scams." Below is a breakdown of the scams that generated the biggest losses:

Type of Financial Scam/Scheme	Global Losses (USD)
Payments Fraud	$386.8B
Credit Card Fraud	$28.6B
Check Fraud	$26.6B

Advance Fee Scams	$19.1B
Cyber-enabled Scams	$10.0B
Impersonation Scams	$6.8B
Employment Scams	$3.9B
Confidence Scams	$3.8B
Total	**$485.6B**

Table 1. Biggest scams of 2023. *Visual Capitalist*

Preventing Fraud – A Shared Responsibility

As a consumer and customer, you can do a lot by arming yourself with knowledge of cybercriminals – what their motivation is, what methods they use, and the tools they use to trick you.

Fraudsters' Motivation. The "Fraud Triangle" states that "individuals are motivated to commit fraud when three elements come together: (1) some kind of perceived pressure, (2) some perceived opportunity, and (3) some way to rationalize the fraud as not being inconsistent with one's values."

Fraudsters are greedy. Self-centered. They do not mind harming or inconveniencing you.

Fraudsters Leverage Human Nature. We each have the right to imperfection – so mistakes will be made. Mistakes may come from poor judgment about taking that "too good to be true" online job offer (with a payment you have to deposit into your bank account right away), or from procrastinating on security application updates to your home PC operating system.

Fraudsters use bots to probe the internet looking for a mistake to exploit. They're sneaky and they're always searching.

Tactics Fraudsters Have Used. Fraudsters use social engineering tactics such as phishing emails, SMS texting, malware, compromised websites, trojans, ransomware, and more.

Fraudsters hope you aren't alert, educated, and smart enough to catch them. Prove them wrong.

Tips To Help You Remain On Guard

- Don’t reveal personal or financial information in a text or email, and don’t respond to email solicitations for this information.
- Don’t click on links sent in a text or email – you might wind up in a scam site built by a cybercriminal.
- Don't send sensitive information over the internet without checking the website's security. Look for URLs that begin with "https" – the ‘s’ stands for secure – rather than "http." A website safety checker like Google Safe Browsing helps, too.

If You’re a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your institution, contact them immediately.

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190