FS-ISAC

C&N

Security Tips Newsletter

September 2023 | Issue No. 2

Security is Everyone's Responsibility

# Be Fraud Wise

## Summary

You've won a lottery that you did not register for. Congratulations! Now if you will only provide us with funds to pay for the taxes up front and provide us with your bank account information…

The tactics found in all fraud scams include the same goal: To obtain your personally identifiable and financial information to steal money. When it comes to fraud, there are no exceptions to the rule.

### Fraud Victim Types

When we think about fraud victim types, Psychology Today states, "Findings in this area are mixed, particularly in terms of education, sex, and race. As for age, some data indicates older people may be at a greater risk of losing more money per fraud incident; nevertheless, victimization rates appear to be highest in the middle-aged age group." There are also other considerations such as a person's awareness and sophistication of the scam.

### Top Fraud Scams

The Consumer Financial Protection Bureau identifies some of the most common types of fraud and scams.

1. Charity
2. Debt collection, settlement, and relief
3. Regulator logo misuse
4. Foreclosure relief, mortgage loan modification
5. Grandparent
6. Imposter
7. Mail
8. Money mule
9. Money Transfer, mobile payment services
10. Lottery
11. Romance

### Prevention Tips

Always exercise caution when it comes to your personal information, banking account information, and online banking credentials. Remember to:

- Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token - a small physical device that can hook onto your key ring. Read Multi-Factor Authentication (MFA) How-to-Guide for more information.
- Use the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts. Read Creating a Password Tip Sheet for more information.

| | |
|---|---|
|  | Practice safe web browsing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection. |
|  | When you find yourself out in the great "wild Wi-Fi West," **avoid** free Internet access with no encryption. |
|  | If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or debit/credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. |
|  | Don't reveal personally identifiable information such as your bank account number, social security number, date of birth, or banking credentials to unknown sources. |
|  | Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email. |

Please remember, if you have had your bank account information stolen or find out that you have been a victim of fraud, report it to your financial institution immediately and visit https://www.usa.gov/where-report-scams and report the matter to the appropriate agency.