

# Live Smart: Be Aware

COMBAT FRAUD AND DON'T BE A VICTIM



# Caveat

- ▶ Everything in this presentation is public knowledge and available to everyone. There are no absolutes in anything anymore, so please use this information strictly as a guide and reminder to use good common sense.
- ▶ This information is being presented as a goodwill gesture by your neighbor as a reminder to remain safe and vigilant. It is not intended as a product or endorsement of any security substitute meant to protect you and your assets.
- ▶ I thank you all for being here and for being good stewards of this community so that we can all live in peaceful setting, in our little corner of the world.

# LIFE

▶ This country will not be a good place for any of us to live in unless we make it a good place for all of us to live in.

▶ Theodore Roosevelt



# Social Engineering Attacks

- ▶ When someone tries to trick you into giving them sensitive information or taking a dangerous action.
- ▶ So much of every day life is performed via electronic means.
- ▶ We work, communicate, and interact mainly through digital means. Our cell phones today are powerful computers capable of many functions. The flip side is they also come with risk.
- ▶ We need to prepare ourselves for this risk and eliminate it or at least mitigate it to the lowest possible denominator.

# Fraud Scams

**"Evil is powerless if the good are unafraid." —President Ronald Reagan**

# Red Flags

When you receive email or notices, check for spelling mistakes, grammar mistakes, strange requests, and personal information to name a few.

Watch to see if the request includes a sense of urgency, fear, or other strong emotion to pressure you into taking quick or immediate action.

If you are asked to respond with an urgent financial request, such as an overdue invoice payment, or large wire transfer, be wary. Verify information by going directly to that company website and do not respond to the email directly.

Stop, look and listen before carrying out and requests

Just one more reminder to remain vigilant.

# Do Not be a victim

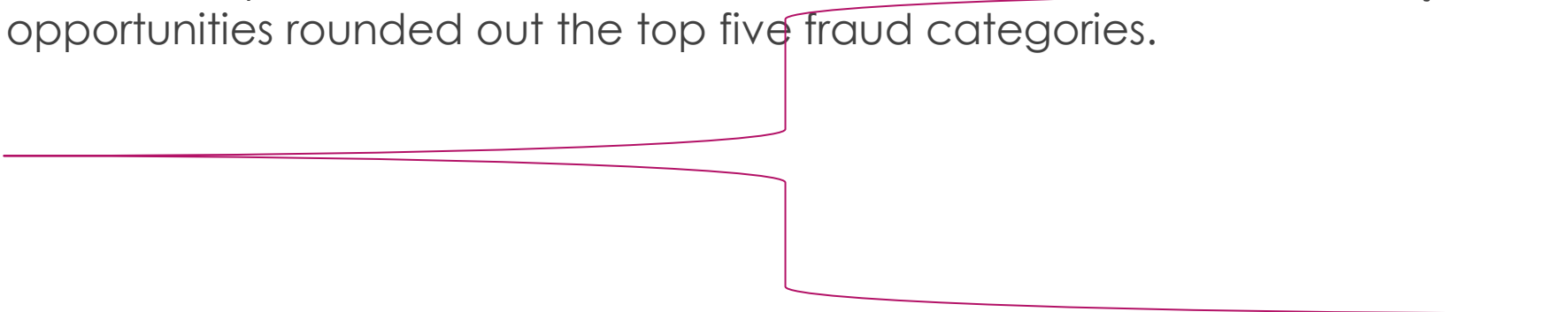
The message of this tutorial is to offer guidance and positivity for each and every one of you.  
The goal is HOPE and confidence: YOU must be vigilant and aware.

# STATISTICS

- ▶ There are many forms of Fraud and Financial schemes in the United States and the world.
- ▶ LIFE is all about mathematics and the predators understand this more than most.
- ▶ In 2021, 5.7 million Americans filed fraud reports. The total dollar impact to this is at least \$5.8 Billion.
- ▶ At least 1 million additional victims did not file reports, so total dollar impact is not known.



# More stats

- ▶ The FTC received fraud reports from more than 2.8 million consumers last year, with the most commonly reported category once again being imposter scams, followed by online shopping scams.
  - ▶ Prizes, sweepstakes, and lotteries; internet services; and business and job opportunities rounded out the top five fraud categories.
- 

# RoboCalls

- ▶ People are getting more robocalls than ever. Technology is the reason: Companies are using auto-dialers that can send out thousands of phone calls every minute for an incredibly low cost.
- ▶ Even if you signed up for DO NOT Call, these calls will still find you and get through.
- ▶ YOU CANNOT hide from these calls, but you can ignore them.
- ▶ WHO IS THEM? Predators
- ▶ JUST don't answer them. If you don't know who the caller number is, then hit "**end call**". They will move onto the next number. They only care about the ones who answer to set their hook. LIFE is mathematics. Send out thousands of calls a day and hope for a 1% or better return and you just made a lot of money.

# SCAM OF THE WEEK:

- ▶ Cybercriminals like to manipulate people into acting on impulse because anyone can fall for this trick, even government officials. In this week's scam, a Russian hacking group is targeting members of the Polish government with an enticing phishing email. The email contains a link that claims to provide information about a mysterious person who has been in contact with Polish government authorities.

If you click it, the link redirects you through multiple websites before reaching an archive of .zip files. This archive contains a malicious file that is disguised as a photograph. If you open the file, a distracting image is displayed while the malicious software secretly downloads onto your device. Once installed, the malware can collect your sensitive data and send it back to the hackers.

# Scam: what to do

- ▶ Follow these tips to avoid falling victim to similar scams:
  - Avoid clicking on links in emails, especially if the email is not expected.
  - Phishing emails may contain alarming or sensitive topics to try and trick you into clicking on a link. Always be mindful any time an email is encouraging you to take action.
- ▶ If an email seems suspicious, always follow your organization's reporting policy. An email that is reported quickly can help to protect your organization from a larger phishing attack.



## SCAM OF THE WEEK:

- ▶ **If something seems too good to be true, it usually is,** and this recent phishing scam is no exception. This week, cybercriminals are sending an email that appears to come from the online retailer XXXX. The sender's email address isn't from a XXXX domain, and the email does not contain any official logos or branding. However, the email claims that you have won a XXXX Mystery Box and encourages you to click a link to claim your prize.

If you click the link, you'll be taken to a website with a URL different from the official XXXX website. You'll be instructed to enter your personal information there so that you can receive the mystery box. Of course, this is a fake website that is controlled by cybercriminals. If you enter your information here, they will be able to steal it immediately.

# Scam: what to do

- ▶ Follow these tips to avoid falling victim to a phishing scam:
  - **Check other sources to verify the legitimacy of an email.** In this case, the email claims that XXXX is giving away a mystery box. If this were a real giveaway, XXXX's official web page would contain more information.
  - Hover your mouse over the link in the email. This action will allow you to see the webpage URL where the link will direct you. In this case, the website URL is not connected to XXXX.
- ▶ Pay close attention to the sender and body of the email. This phishing email sender doesn't appear to be related to XXXX. The body of the email doesn't contain logos or branding, meaning that it is unlikely to be an official email.

## SCAM OF THE WEEK:

### Fake Login Fiasco

- ▶ Scammers frequently try to trick you into clicking on malicious links in emails by making them appear legitimate. In a recent scam, they are trying to trick you with an email that appears to be related to your Microsoft account security. The email says that there has been some unusual activity on your account and that many of your account's features have been locked. There is a link in the email, along with instructions to click it so that you can review all activity on your account.

If you click the link, you'll be taken to what appears to be a Microsoft login page. However, the login page is actually fake, and you won't be taken to your Microsoft account if you enter your login information here. Instead, entering your user credentials on this page will allow cybercriminals to steal them. Once they have your username and password, they can use them to access your account and steal your personal information.

# Scams: what to do

Follow these tips to avoid falling victim to a phishing scam:

- Scammers will often try to scare you into acting impulsively. Always stop and think before clicking, especially if an email is instructing you to act quickly.
- Pay attention to the details of the email. Phishing emails will often contain spelling and grammatical errors, or the wording of the email may seem unusual.

Navigate to the official website in your browser whenever possible. Clicking a link in an email may direct you to a fake or malicious website.



# Scam of the Week: Travel Offers too good to be true

In this week's scam, cybercriminals are taking advantage of travelers and tourists by sending out fake emails. The emails appear to be from legitimate airlines, hotels, and other travel-related organizations. However, the emails are actually a clever trick that scammers use to steal your money and personal information.

The email you receive could appear to be from any travel organization, and they usually offer a chance to win a prize or a travel package. Or the email may sound urgent, such as claiming that you need to resolve an issue with your Airbnb or hotel account. If you click the link in one of these emails, you will be taken to a fake website and instructed to enter your personal information or user credentials. Anything you enter on these fake websites is transmitted directly to the cybercriminals. You do not win a prize for following the instructions in the emails, but the cybercriminals do. They get your data!

# Scam: what to do

Follow these tips to avoid falling victim to travel scams:

- Be skeptical of email offers that sound too good to be true.
- **Unsolicited emails that instruct you to take an urgent action should be treated very cautiously.** Cybercriminals often try to create a sense of urgency to trick you into falling for their scams.

Legitimate travel organizations will not ask you to provide sensitive or personal information through email. Always make sure that you are using the organization's official webpage before entering any information or user credentials.

# Identity theft

- ▶ Fraud using Identity theft is the most common type that people encounter. Over the past 30 years, this type crime has grown exponentially. It is extremely important to report this crime to cover yourselves financially and from civil risk. Reporting these crimes allows law enforcement to keep tracking records of the activities to assist in lengthy investigations.
- ▶ Please understand that this type crime is extremely difficult to investigate on the local level due to jurisdiction, lack of information and highly restrictive access to records, even if the records are yours.

# Identity Theft cont'd.

The onus for this type of crime is strictly on the victim. It is imperative to keep good records and have them available to the police.

You will need a copy for your records and a copy for the police.

The police will then have to subpoena your records from the Bank to ensure that they are the certified original records, but your copies can move the investigation forward in a much quicker time.



# Identity Theft

This is a newer phenomenon crime to law enforcement. It is a specialized field with few investigators on the local level. This crime has blossomed over the past 30 years to what it is now and you have to remain vigilant.

DO NOT be surprised if the police officer does not know or tries to tell you there is nothing they can do. It is because they lack the experience and knowledge to investigate these lengthy, exhaustive, and complicated investigations. They also do not have the time and resources available to them. Remain calm and just ask them to take the initial information and evidence and please begin an information/fraud report so that the process can begin. Make sure you have your documentation and records available with a copy for yourself.

# Identity Theft

The sooner the information enters into the law enforcement system, the sooner the investigation can begin.

You play a **CRITICAL** role in this process. It is imperative that you remain vigilant with all of your accounts (Bank and credit cards, home mortgage, retirement accounts, etc.)

If at anytime, you become overwhelmed with finances, it would be most wise to retain the services of an attorney and/or wealth manager for advice and possible assistance with your accounts to further protection.

# Identity Theft

If you retain the services of a wealth manager/financial advisor, et al, make sure they are licensed, bonded and attained the status of a fiduciary professional. It is also best if they only specialize in this field of finance and finance law to best protect you and your investments.

# Identity Theft

It may also be a smart investment to protect yourself with one of the certified theft protection services offered on line and with your banks.



# Federal Trade Commission (FTC)

As the nation's consumer protection agency, the FTC takes reports about scammers that cheat people out of money and businesses that don't make good on their promises. We share these reports with our law enforcement partners and use them to investigate fraud and eliminate unfair business practices. Each year, the FTC also releases a report with information about the number and type of reports we receive.

[ReportFraud.ftc.gov](https://ReportFraud.ftc.gov)



# Federal Bureau of Investigations (FBI)

To report fraud or scams to the FBI :

1. Contact the FBI at (202)324-3000
2. Report online at [www.fbi.gov](http://www.fbi.gov)

# Reporting Financial Fraud

- **Gather information about the fraud.** Before you start your report, make sure all the information or evidence you have is at hand and readily available. Make copies of any original documents so you can send the copy and retain the original unless instructed otherwise. If you're filing a report online, you will want to make digital copies of your documents, which may include scanning the original document or taking screen shots.
- Information or documents that might be useful to investigators include any emails or letters you've received related to the fraudulent activity, bills, and account statements.

# Report fraud

- **Visit the [stopfraud.gov](https://www.stopfraud.gov) website.** The website is run by the federal government's Financial Fraud Enforcement Task Force, which coordinates efforts of several federal law enforcement agencies including the FBI to combat financial fraud.
- The task force was created in November 2009 in the wake of the financial crisis, and aims to investigate and prosecute financial crimes across all sectors and financial markets.
- While you may think of crimes such as identity theft and credit card fraud, financial fraud also encompasses corporate fraud, predatory lending, securities fraud, procurement and insurance fraud, and other types of illegal financial activities.

# Report Fraud

- **Categorize the type of fraud you want to report.** After you click on the tab to report fraud, you will find a list of a number of different types of financial fraud handled by different federal agencies.
- The task force includes more than 20 federal agencies, U.S. attorney's offices, and various state and local law enforcement agencies, and has a broad mission.
- In many cases the situation you want to report may fall under more than one category. For example, if someone attempts to steal your credit card or bank account information online, this could constitute identity theft as well as computer-based fraud or cyber crime.
- If the incident you want to report falls under more than one category, you should consider reporting the fraud under both categories. Different agencies may be involved depending on the subject matter of your report



# Live Smart

- ▶ **"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel." —Maya Angelou**