A GUIDE TO AVOIDING ONLINE SCAMS

BROUGHT TO YOU BY DAILY CALLER PATRIOTS

Cybercriminals are becoming increasingly present in today's digital landscape. As technology advances at unprecedented levels, scammers are becoming more difficult to track down.

It is estimated that 4.66 billion people use the internet in 2021, or roughly 60% of the total global population. The number of internet users are growing at an astounding 7% annually. This is equivalent to 875,000 new users each day.

Who is most at-risk for cybercrime?

Every year, scammers steal $40 billion from seniors in the United States.

According to Javelin Strategy & Research, more than 1 million children under the age of 18 were victims of cybercrime in 2017, specifically identity theft.

Children and seniors are considered targets for online scammers. That is why it is imperative to understand the nature of cybercrime and the steps you can take to prevent it.

TIPS TO AVOID ONLINE SCAMS

Once you've given your password to someone, there's no way to tell who else may have it.

Only give out your personal information when you know the source is trusthworthy.

1

Make sure your method of payment is secure

When a Url starts with HTTP instead of HTTPS, chances are it is not a secure site.
Avoid entering methods of payment that are direct transfers to your bank account.
Using credit cards with fraud protection is optimal.

2

Be aware of clones

In this digital age, scammers often impersonate other figures, essentially acting as their clone.
Be wary of typos or bizarre speech patterns.
Pay attention to the email being used.
Scammers may alter email addresses to mimick real ones.

3

What to do if you fall victim to a scam

Sometimes, unfortunate things happen at no fault of your own. However, there are steps you can take to protect yourself.

If you know a scammer has gotten hold of your credit or debit information, contact your bank and credit card company directly. Depending on your specific situation, you can ask to simply cancel your credit card. If matters appear to be dire, your bank can close your bank account for you. If money has been charged to your card or taken out of your account, you should try to work with your bank to get a refund.

What to do if you fall victim to a scam

Sometimes, unfortunate things happen at no fault of your own.
However, there are steps you can take to protect yourself.

If your device has been infected with ransomware, please take it to a professional who can detox the software. If you try to fix it on your own, things may get worse, resulting in extreme software damage.

have the professional change your online information (usernames, passwords) to make it harder for scammers to reach you.

What to do if you fall victim to a scam

Sometimes, unfortunate things happen at no fault of your own.
However, there are steps you can take to protect yourself.

So you've accidentally given private information such as your social security number or credit card number to scammers.

Now what?

You're now more likely to fall victim to identity theft. Watch your credit statement to make sure no suspicious charges appear. Remember, you can always cancel your credit card. If you know you are a victim of identity theft, please contact the FTC.

TOP SCAMS TO WATCH OUT FOR

1 PHISHING SCAM

WHEN A SCAMMER IS TRYING TO GET THEIR HANDS ON YOUR PRIVATE INFORMATION (PASSWORDS, USERNAMES, CREDIT CARD INFORMATION) THROUGH IMPERSONATION

2 DEBT RELIEF

SCAMMERS ARE MORE LIKELY TO CARRY OUT THIS SCHEME IF THERE IS WIDESPREAD FINANCIAL HARDSHIP. THEY WILL PRETEND TO BE CREDIT OR FINANCIAL INSTITUTIONS OFFERING YOU WAYS TO GET RID OF DEBT. IF SOMEONE YOU DON'T KNOW CONTACTS YOU WITH A SIMILAR CLAIM, PLEASE DO YOUR RESEARCH BEFORE TRUSTING THEM.

3 ROMANCE SCAM

SCAMMERS WILL OFTEN PREY ON THE EMOTIONALLY WEAK. IF SOMEONE YOU DO NOT KNOW BEFRIENDS YOU ONLINE, THEY MAY EVENTUALLY ASK FOR MONEY. DO NOT FALL FOR THIS TACTIC.

TOP SCAMS TO WATCH OUT FOR

TECHNICAL ISSUE

4

SCAMMERS WILL OFTEN PRETEND TO BE CUSTOMER SUPPORT NETWORKS AND CONTACT YOU CLAIMING THERE ARE ISSUES WITH YOUR ACCOUNT BEFORE ASKING FOR YOUR CREDIT CARD NUMBER. THIS IS OFTEN FAKE, BE VERY WARY OF SUCH SCHEMES.

FREE OFFERINGS

5

BAD GUYS WILL OFFER TO GIVE YOU FREE THINGS IN EXCHANGE FOR YOUR PERSONAL INFORMATION. THIS IS A COMMON TACTIC FOR THOSE WHO DESIRE TO COMMIT IDENTITY THEFT.

ACCIDENT SCAM

6

YOU MAY RECEIVE A CALL FROM AN UNKNOWN NUMBER SAYING A LOVED ONE HAS BEEN IN A CAR ACCIDENT. THIS IS VERY COMMON. UNLESS YOU GET THIS CALL FROM SOMEONE YOU TRUST, IT IS ALMOST ALWAYS A SCAM.

TOP SCAMS TO WATCH OUT FOR

7

RANSOMWARE SCAM

SOMETIMES, SCAMMERS MAY SEND YOU EMAILS OR POP-UP MESSAGES WITH LINKS OR ATTACHMENTS THAT ARE EMBEDDED WITH RANSOMWARE. RANSOMWARE MAY TAKE OVER YOUR COMPUTER AND LOCK YOU OUT OF YOUR SYSTEM. IF YOU RECEIVE A SUSPICIOUS EMAIL ASKING YOU TO DOWNLOAD SOMETHING, DO NOT CLICK ON IT.

8

REFUND SCAM

YOU MAY HAVE BEEN SCAMMED BEFORE AND WERE PROMISED GOODS OR SERVICES YOU NEVER RECEIVED. REFUND SCAMMERS WILL CLAIM TO 'REFUND' YOU FOR THAT MISHAP, JUST TO STEAL YOUR INFORMATION AND MONEY AGAIN.

9

GOVERNMENT IMPERSONATION SCAM

SCAMMERS MAY PRETEND TO BE FIGURES OF AUTHORITY TO CLAIM YOUR MONEY.

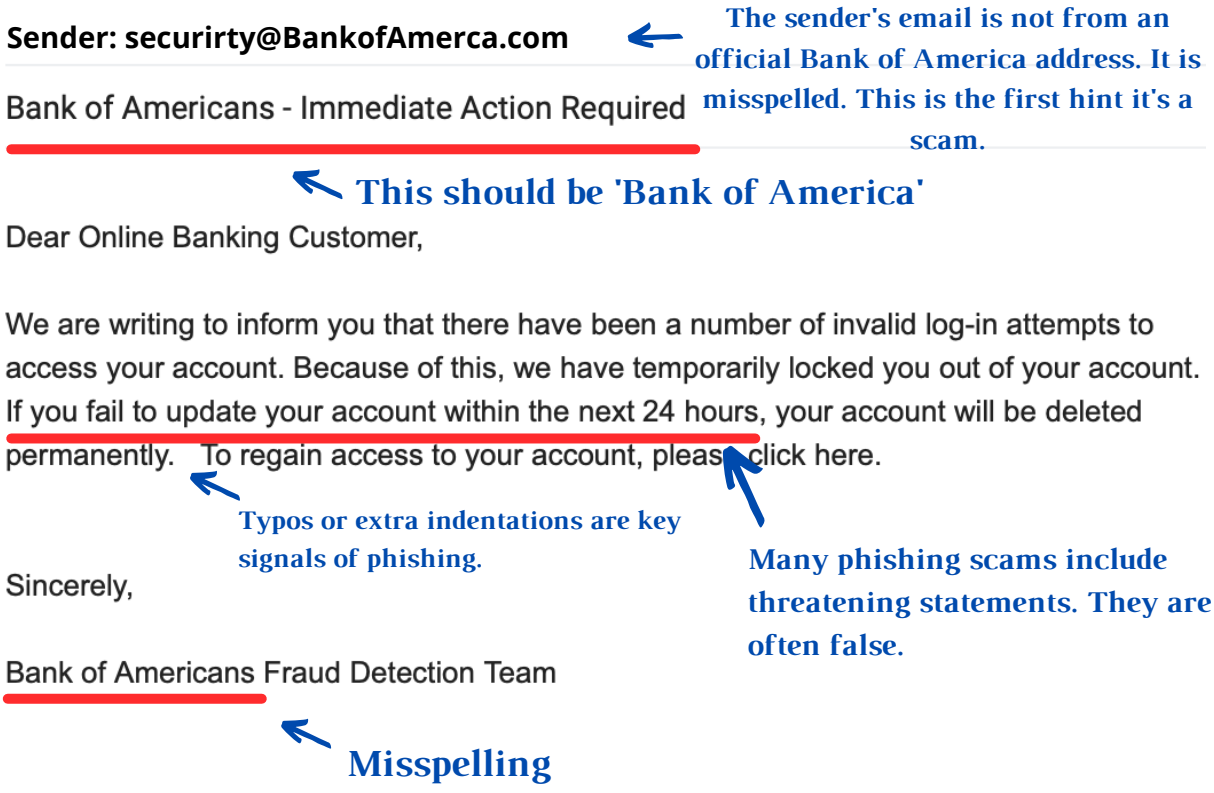
Phishing Scams

THROUGH FAKE TEXT MESSAGES, EMAILS, AND PHONE CALLS, FRAUDSTERS WILL TRY TO GET YOU TO GIVE UP IMPORTANT PERSONAL INFORMATION SUCH AS:

- BANK ACCOUNT INFORMATION
- CREDIT CARD NUMBERS
- SOCIAL SECURITY

How To Recognize Phishing Scams

This is an example of scammers pretending to be part of the "fraud detection team" at Bank of America. The graphic below shows key indicators of phishing scams: misspellings and typos. If links or attachments are embedded within the message, do not click on them. If you are unsure if the message you received is real, you should contact a trusted number or email of the supposed company.



Debt Relief Scams

WHILE THERE ARE CERTAIN COMPANIES THAT CAN HELP YOU RELIEVE YOUR DEBT, MANY SCAMMERS WILL TRY TO POSE AS A LEGITIMATE SOURCE AND OFFER TO CANCEL YOUR DEBT QUICKLY.

WARNING SIGNS OF DEBT RELIEF SCAMS:

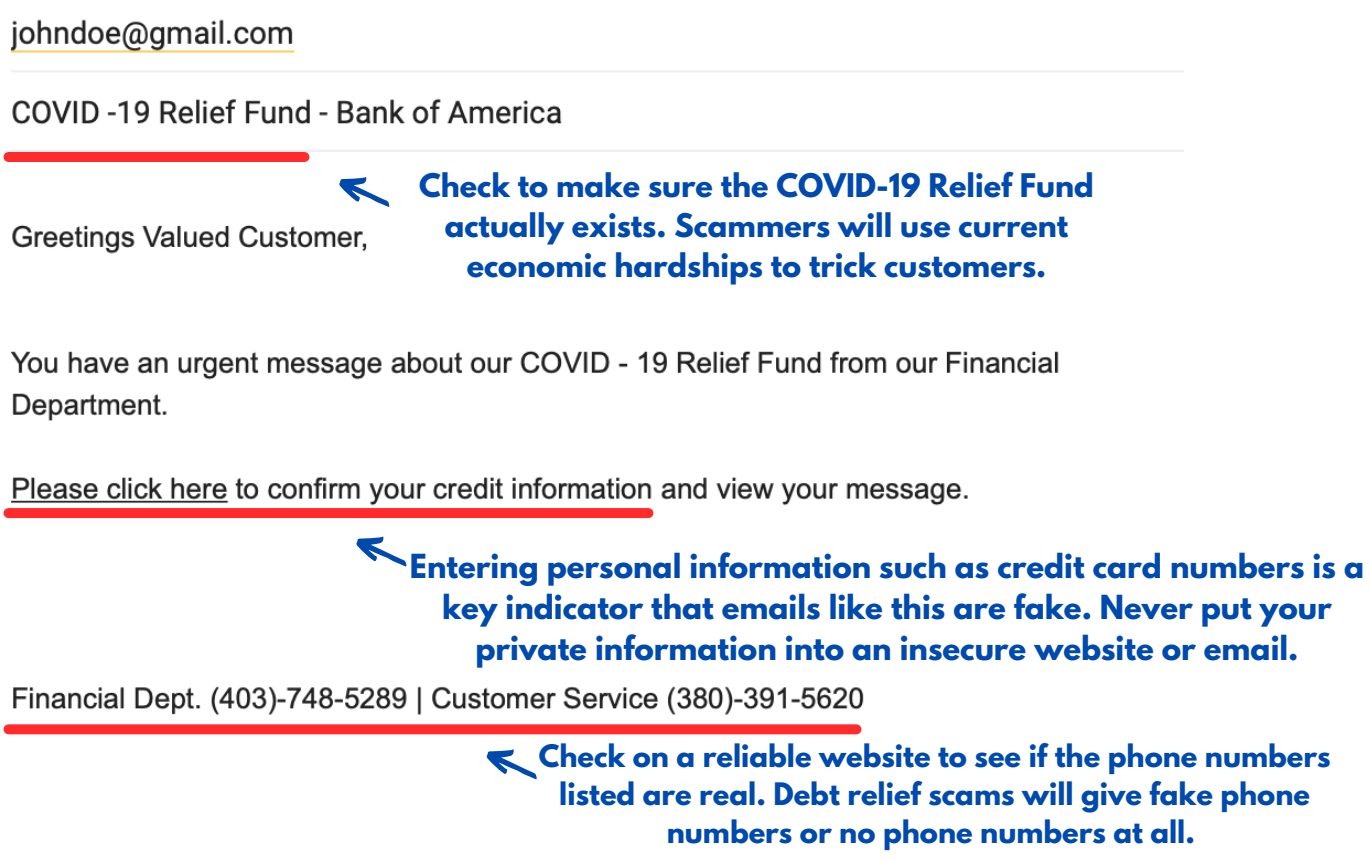
THEY WILL NOT RELAY ANY INFORMATION CONCERNING THEIR SERVICES UNLESS YOU GIVE YOUR CREDIT OR BANKING NUMBERS

ASKS FOR FEES UPFRONT PRIOR TO REPAIRING DEBT

TELLS YOU TO CUT OFF COMMUNCIATION WITH CREDITORS

How To Recognize Debt Relief Scams

This is a classic example of a debt relief scam. They are promising you unknown COVID - 19 Relief information in exchange for your credit and banking information. Many times, these scammers will also threaten to shut down your 'account' or credit cards if you do not give them the information they want. This is almost always fake. If you are concerned call a trusted bank or credit institution number and ask them about the subject of said email. If you're sure the email is a scam, please report them to the FTC here.



Check to make sure the COVID-19 Relief Fund actually exists. Scammers will use current economic hardships to trick customers.

Entering personal information such as credit card numbers is a key indicator that emails like this are fake. Never put your private information into an insecure website or email.

Check on a reliable website to see if the phone numbers listed are real. Debt relief scams will give fake phone numbers or no phone numbers at all.

Romance Scams

HERE ARE SOME QUICK FACTS REGARDING ROMANCE SCAMS:

IN 2018, THE MAJORITY OF ALL SCAMS REPORTED TO THE FEDERAL TRADE COMMISSION (FTC) WERE ROMANCE SCAMS.

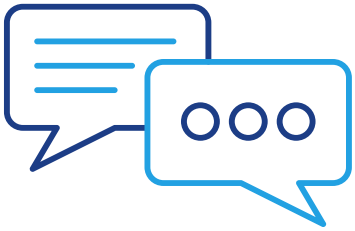
SINCE 2015, REPORTED LOSSES FROM ROMANCE SCAMS HAVE QUADRUPLED

IN 2019, MORE THAN 25,000 CUSTOMERS REPORTED FALLING VICTIM TO A ROMANCE SCAM, AMOUNTING IN $201 MILLION IN DAMAGES. (FTC)

Key Characteristics Of Romance Scams

The perpetrator will try to get close to you quickly without having met in person.

You find them asking many questions about your personal life without telling you much about themselves.



The scammers will try to convince you that they need money for emergencies, medical needs, or travel expenses. Do not give them any of your private information and report them to the FTC.

Technical Scams

IF YOU HAVE A COMPUTER, CHANCES ARE YOU'VE BEEN CONTACTED BY UNKNOWN NUMBERS CLAIMING TO REPRESENT TECHNICAL SUPPORT SERVICES LIKE MICROSOFT, APPLE, ETC.

THEY WILL TRY TO GET YOU TO DOWNLOAD SUSPICIOUS THIRD-PARTY SOFTWARE TO HELP WITH YOUR 'TECHNICAL ISSUES'. THIS WILL ALLOW THEM TO HAVE REMOTE ACCESS TO YOUR COMPUTER. MEANING, THEY WILL HAVE TOTAL CONTROL OVER YOUR COMPUTER.

THEY WILL NOW ASK FOR A METHOD OF PAYMENT. IF YOU REFUSE TO PAY, THEY COULD BLOCK YOU OUT OF YOUR COMPUTER, STEAL BANK INFORMATION, OR WORSE AS THEY NOW HAVE ACCESS TO ALL OF YOUR PASSWORDS AND PERSONAL INFORMATION.

How To Recognize Technical Scams

Though technical support scams nowadays often occur via computer like the example above, you may also receive a 'spam' call from an unknown number trying to gain access to your private information. If you pick up a scam call, block the number immediately and report to the FTC.

If you see a message on your home screen like the one above, try to 'x out' of it as soon as possible. If you can't try to restart your computer. If this still is not working, take your computer to a professional who can help you.

Free Offering Scams

WHO DOESN'T LOVE GETTING FREE THINGS? WHILE FREEBIES MAY SOUND ENTICING, YOU HAVE TO BE CAUTIOUS OF WHERE YOU'RE PUTTING YOUR PERSONAL INFORMATION. IF YOU HAVE TO PUT IN YOUR CREDIT CARD INFORMATION FOR SHIPPING AND HANDLING YOUR 'FREEBIE' IS MOST LIKELY A SCAM.

WARNING SIGNS OF FREE OFFERING SCAMS:

IF YOU HAVE TO PUT IN YOUR CREDIT CARD INFORMATION FOR SHIPPING AND HANDLING YOUR 'FREEBIE' IS MOST LIKELY A SCAM.

THE MAJORITY OF FREEBIES ARE ONLY WORTH A FEW BUCKS. IF THE COMPANY IS OFFERING YOU A GIFT CARD OR OTHER PRODUCTS WORTH MORE THAN A FEW BUCKS, IT IS ALMOST ALWAYS A SCAM.

How To Recognize Free Offering Scams

The example above demonstrates a typical freebie scam. The supposed company is offering a free service in exchange for 'processing fees'. If you were to fill in this link with your credit card information, the company will now have your information on file at their disposal. If you're unsure if the offer is legit, check on Netflix's website. If there's nothing listed, it's most likely fake. You may also report these scammers to the FTC here.

Accident Scams

IF YOU'VE RECEIVED SPAM CALLS SAYING YOUR FAMILY MEMBERS HAVE BEEN IN A BAD ACCIDENT AND YOU NEED TO GIVE UP YOUR CREDIT CARD INFORMATION TO PAY FOR MEDICAL BILLS, YOU'RE NOT ALONE.

ESSENTIALLY, SCAMMERS ARE CREATING FAKE EMERGENCIES TO GET YOUR MONEY

How To Recognize Accident Scams

YOU MAY GET CALLS, TEXTS, EMAILS, OR SOCIAL MEDIA MESSAGES FROM THESE FRAUDULENT FIGURES. THEY MAY PRETEND TO BE FIGURES OF AUTHORITY LIKE POLICE, FEDERAL AGENTS, DOCTORS, NURSES. THEY ARE ALSO KNOWN TO ACT LIKE FRIENDS AND FAMILY.

IF YOU DO NOT RECOGNIZE THE NUMBER OR EMAIL ADDRESS, CALL A FAMILY MEMBER OR TRUSTED FRIEND TO SEE IF WHAT THE SCAMMER IS PROPOSING IS ACTUALLY TRUE. DO NOT WIRE MONEY TO THEM, AND REPORT THE NUMBER TO THE FTC.

Maybe: Unknown Number

Your grandson, John, has been in a severe car accident. He is in critical condition.

Please call this number to immediately pay for his urgent hospital bills:

(483)-475-1278

Ransomware Scams

SCAMMERS MAY TRICK YOU INTO DOWNLOADING RANSOMWARE ONTO YOUR COMPUTER. THIS MALWARE WILL LOCK YOU OUT OF YOUR COMPUTER AND DEMAND YOU PAY A 'RANSOM' TO GET YOUR COMPUTER BACK. IF YOU PAY, THE SCAMMER NOW HAS YOUR PRIVATE INFORMATION AND YOUR COMPUTER WILL LIKELY NOT BE UNLOCKED.

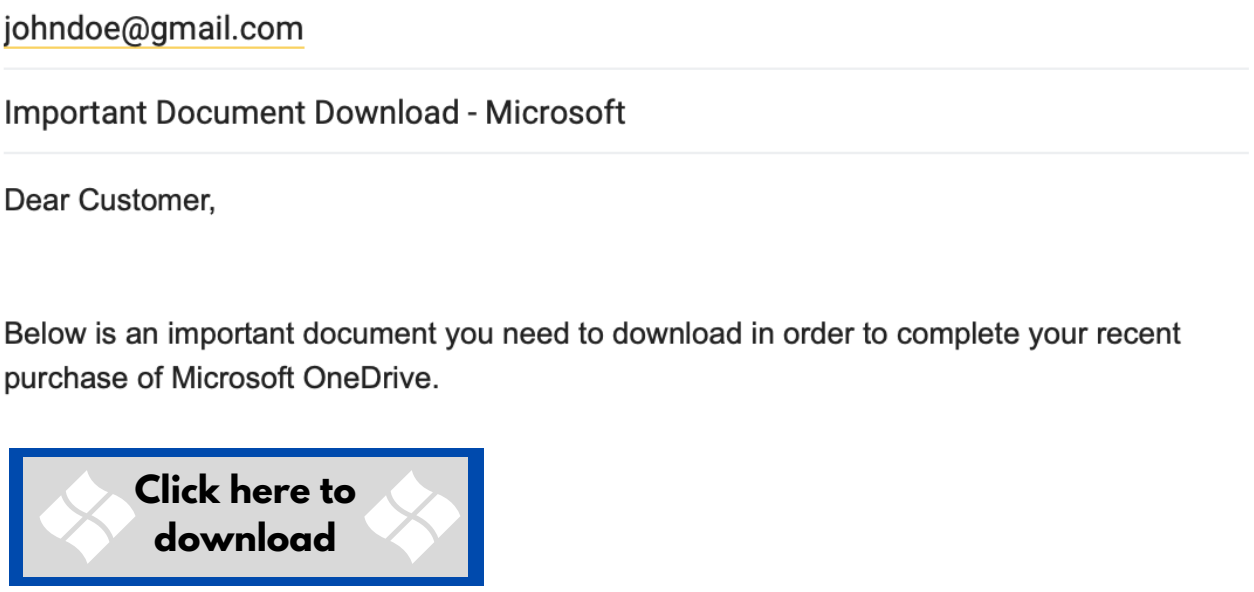
HERE ARE SOME WARNING SIGNS OF RANSOMWARE SCAMS:

YOU GET AN EMAIL OR TEXT SAYING IN ORDER TO VIEW THE CONTENTS OF THE MESSAGE, YOU NEED TO DOWNLOAD SPECIAL SOFTWARE.

POP-UP BOXES START APPEARING ON YOUR HOME SCREEN WITH VARIOUS OFFERS TO ACCESS PAID SITES FOR FREE IF YOU DOWNLOAD SPECIFIC SOFTWARE.

How To Recognize Ransomware Scams

In this situation, you would not click the attachment and report them to the FTC. You can also try to block the address so they can't contact you anymore. Here are some ransomware software that is known to be dangerous. AVOID THESE AT ALL COSTS:
WannaCry, Bad Rabbit, Locky, Troldesh, CryptoLocker, Petya, and Ryuk



johndoe@gmail.com

Important Document Download - Microsoft

Dear Customer,

Below is an important document you need to download in order to complete your recent purchase of Microsoft OneDrive.

Click here to download

Thank you,

Microsoft
The Microsoft OneDrive Team

Refund Scams

IF YOU'VE FALLEN VICTIM TO AN ONLINE SCAM IN THE PAST, YOU'RE MORE LIKELY TO BE TARGETED BY A REFUND SCAM BECAUSE SCAMMERS ALREADY HAVE YOUR INFORMATION. THESE SCAMMERS WILL PROMISE A GOOD OR SERVICE TO MAKE UP FOR THE MONEY YOU LOST PREVIOUSLY.

STEPS YOU CAN TAKE TO MAKE SURE YOU DON'T FALL VICTIM:

DO NOT GIVE YOUR MONEY OR PERSONAL INFORMATION VIA EMAIL, CELLPHONE, OR ANY OTHER ELECTRONIC MESSAGING PLATFORM IF YOU'RE TOLD YOU HAVE TO PAY A FEE.

IF SOMEONE TELLS YOU THEY'RE FROM A US GOV. AGENCY, THAT IS UNTRUE. HANG UP THE PHONE AND REPORT THEM TO THE FTC. GOV. AGENCIES WILL NOT CALL YOU. ADDITIONALLY, GOV. AGENCIES WILL OFTEN NOT CHARGE FEES FOR THEIR SERVICES.

How To Recognize Refund Scams

One of the most common types of refund scams is a fake tax refund. Below, we've made a mock-up of what a potential fake tax refund scam may look like. In this example, the IRS is contacting the customer to tell them they are eligible for a tax return. In reality, the IRS will not contact you. If you receive a message like this, it is fraudulent. Immediately report the sender to the FTC so others do not get scammed.

johndoe@gmail.com

Tax Refund Eligibility - Internal Revenue Service

Dear Eligible Taxpayer,

Never click an attachment in an email. This tax return is fake, so the attachment will most likely take you to a suspicious server that will steal your private info.

After analyzing your recent tax filing for the fiscal year of 2019, our department has determined that you are eligible for a tax return.

To claim your money, you can place a tax return request by clicking here. Once you click this link, please enter a valid credit or debit card to fast-track your request.

If you enter your info. it will be stored on their fraudulent servers for future scams.

If you have any questions, please contact us at (387)-859-9375

The scammers may give you a number to call. This probably will be a fake number to seem more legitimate.

Regards,

The Internal Revenue Service Team

| 2647 Consitution Ave, Washington, D.C. 20006 |

Government Impersonation Scams

GOVERNMENT IMPERSONATION SCAMS INVOLVE SCAMMERS TRYING TO POSE AS AUTHORITY FIGURES TO GET YOUR MONEY. ACCORDING TO THE INTERNET CRIME COMPLAINT CENTER (IC3), MONETARY LOSSES FROM THIS TYPE OF SCAM TOTALED $124 MILLION IN 2019.

HERE ARE SOME SIMPLE STEPS YOU CAN TAKE TO PREVENT THIS SCAM:

DO NOT PLACE YOUR TRUST IN THE PERSON CALLING. MANY SCAMMERS WILL FAKE THEIR CALLER ID TO LOOK LEGITIMATE.

FAKE DEBT COLLECTORS WILL TRY TO GET YOU TO WIRE MONEY VIA CHECK, ONLINE PAYMENT, CREDIT, OR DEBIT CARD. NEVER DO IT, THE IRS WILL NOT CONTACT YOU VIA PHONE TO COLLECT DEBTS.

PUT YOUR NAME ON THE NATIONAL DO NOT CALL REGISTRY. THIS WILL PREVENT LEGITIMATE SALES COMPANIES FROM CALLING YOU. THAT WAY, YOU'LL KNOW THE COMPANY CALLING YOU IS FRAUDULENT, AS THEY DON'T HONOR THIS REGISTRY.

How To Recognize Gov. Impersonation Scams

FBI | Police Scammers

There is a warrant out for your arrest because you failed to appear in court for your traffic violation. Click here for more information:

www.sheriffdccounty.com/traffic

Social Security Scammers

Your social security number has been compromised. If you do not click on this link within 48 hours, your social security will be terminated:

www.ssgov.com/social/fix/security

IRS Scammers

There has recently been a claim filed against you. In 2019, you did not report your taxes. Click here for further information regarding the lawsuit:

www.irs.com/file/claims

Healthcare Scammers

In times of COVID-19, the department of health and human services is giving away free COVID self-tests. Claim yours here:

www.healthgov.com/covid/relief/tests

If you receive a message like this, please report the number or email to the FTC by clicking here.