Don’t Get Slammed By Job Scams

Jennifer Weggeman

VIRTUAL JOB CLUB

workNet DuPage
americanjobcenter

workNet DuPage
americanjobcenter

Workforce Innovation & Opportunity Act (WIOA GRANT)

- **Virtual Job Club - Open to Public**
- **Job Search Workshops (Registered Clients)**
- **Training Grants- up to $10,000 (Registered Clients)**
- **<u>*Layoff to Launch workshop every Tuesday*</u>**

Visit our Website for Application and to sign up for the events:

www.worknetdupage.org

workNet DuPage
americanjobcenter

WHAT WE WILL COVER TODAY

- JOB SCAMS AND WHY YOU NEED TO KEEP YOUR ANTENNAE UP
- FEAR AND UNCERTAINTY OF COVID-19 HELPS SCAMMERS
- RESOURCES TO LEARN HOW TO STAY SAFE AND AVOID GETTING SLAMMED

LOOKING FOR A JOB? LOOK OUT FOR SCAMMERS!

Scammers might promise you a job, lots of money, or work you can do at home.

They might also charge you before they help you. Did you know you should never pay somebody to help you find a job?

If you pay them, you will lose your money and will not get a job through them.

workNet DuPage
americanjobcenter

JOB SEEKERS ARE TARGETED

Many people, due to social/cultural programming, will comply with orders for information and provide Personal Private Information (PPI) details without questioning source:

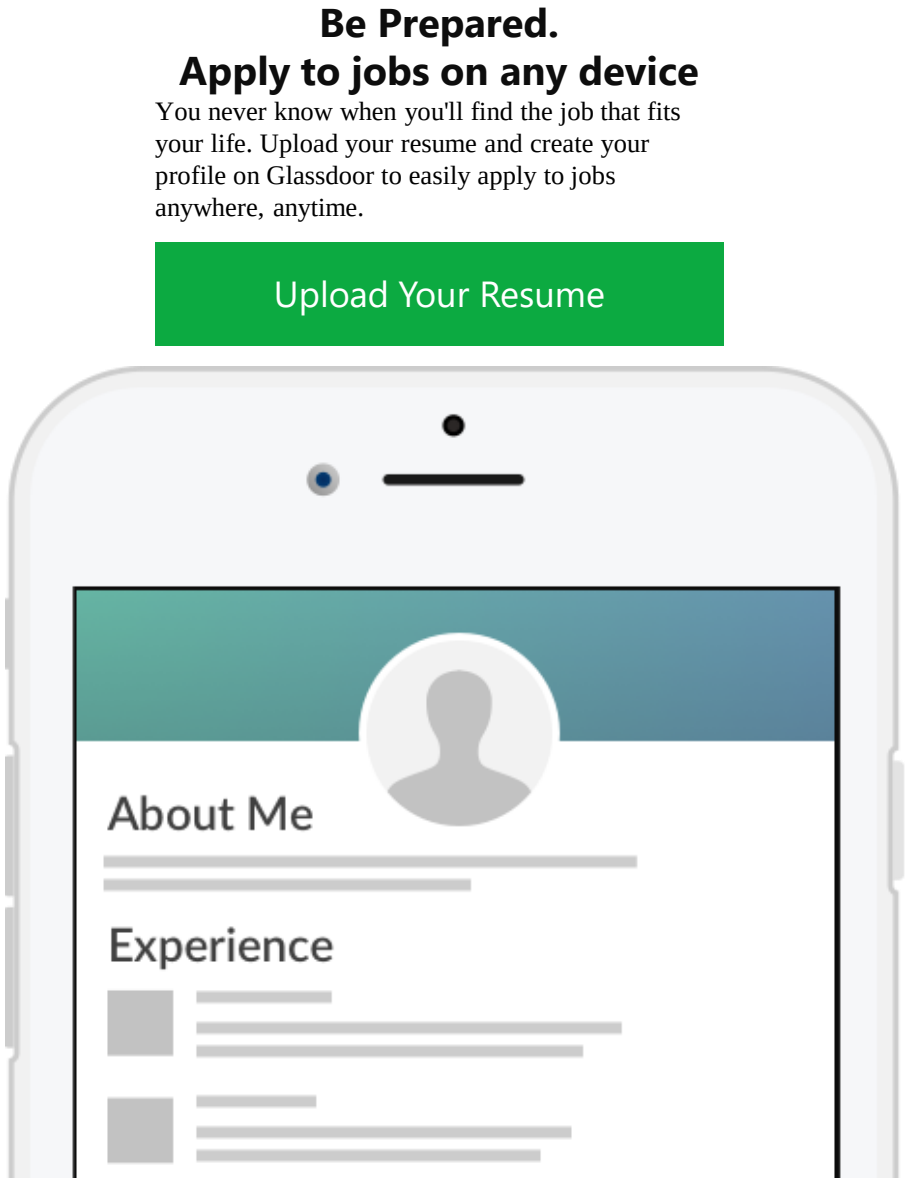
- ❑Social Security Number
- ❑Address, Phone and Date of Birth
- ❑Bank & Account info

TMI on social media

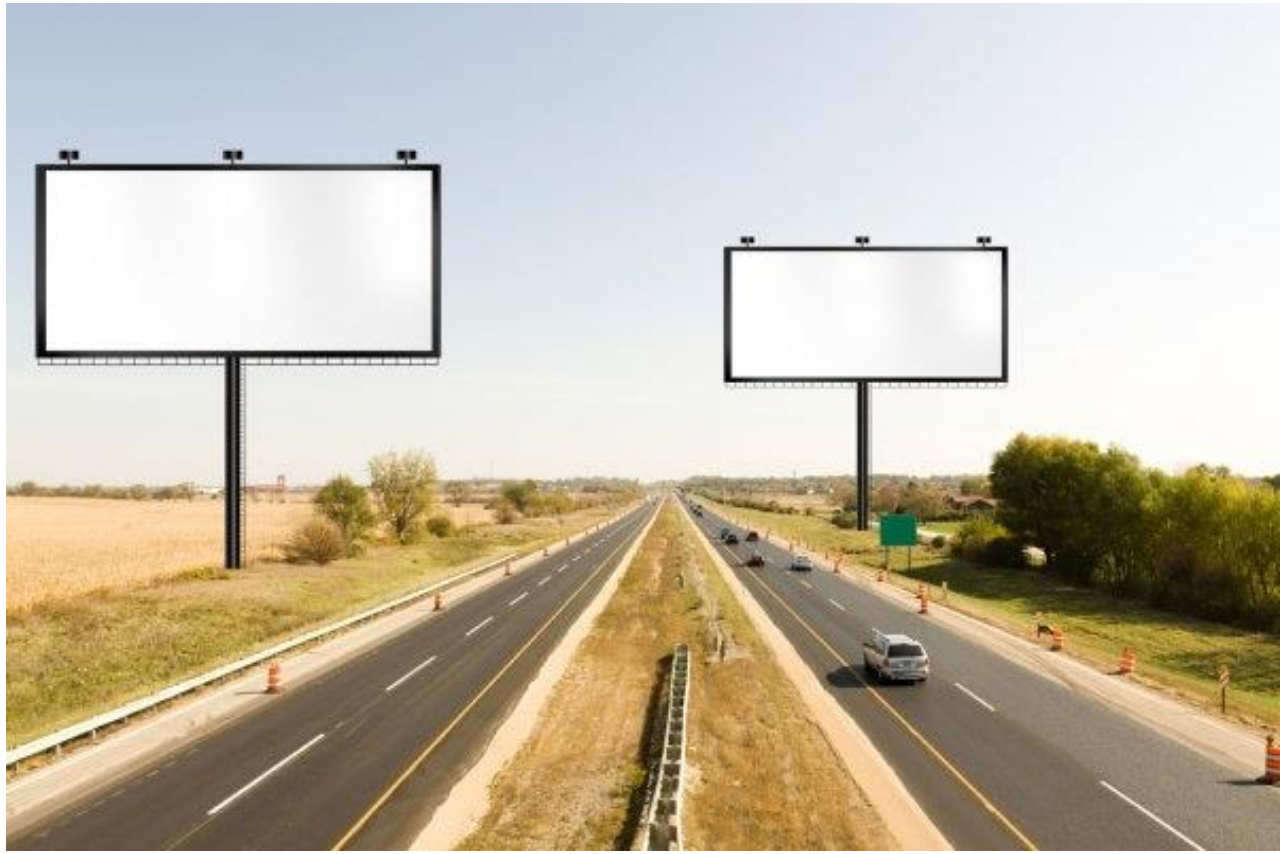
workNet DuPage
americanjobcenter

JOB SEEKERS ARE TARGETED

- ❑Actively looking for legitimate opportunities
- ❑You have uploaded your resume on multiple job boards and websites
- ❑Easily available to reach by phone and email
- ❑Talking with many different people, can let your guard down

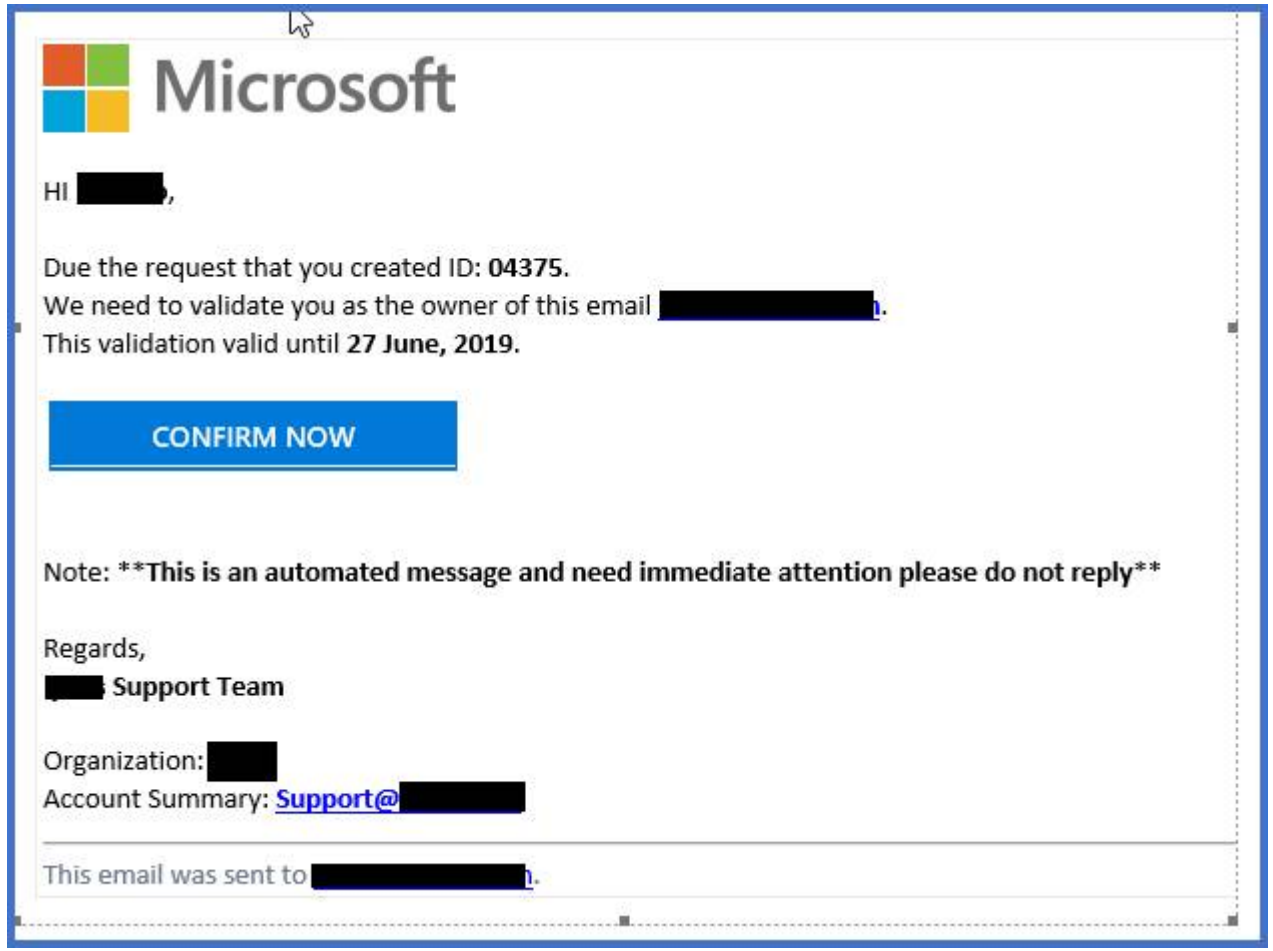


Remember during job search, if you are posting info on platforms like LinkedIn, FaceBook, Twitter, Job Boards, you are letting ANYONE see your data, photos and uploaded files (resumes) unless you **change the open default settings to more private option settings.**



workNet DuPage
americanjobcenter

New Job? Don't be the new hire that takes down the whole network!



Microsoft

HI [redacted],

Due the request that you created ID: **04375**.
We need to validate you as the owner of this email [redacted].
This validation valid until **27 June, 2019**.

CONFIRM NOW

Note: **This is an automated message and need immediate attention please do not reply**

Regards,
[redacted] **Support Team**

Organization: [redacted]
Account Summary: Support@[redacted]

This email was sent to [redacted].

Organizations are dealing with phishing emails. In fact, research shows that **between 86% and 91% of all data breaches start with an employee responding to a phishing email.** This phishing attempt was seen in an organization.

Please be aware that Microsoft will never send you an email asking you to do anything to keep your email account active, or to validate your email account. If you see emails like the one below, please do not respond to them and delete them immediately.

EMPLOYMENT SCAMS

EXAMPLES OF SCAMS REPORTED RECENTLY

Indeed Job Scam

Texas Man claims job search on Indeed led to $2000 Scam

https://abc7chicago.com/man-claims-job-search-led-to-$2000-scam/5255320/

Fraud Scam Maps

https://www.bbb.org/scamtracker

https://action.aarp.org/site/SPageNavigator/FraudMap.html

workNet DuPage
americanjobcenter

PROTECT YOURSELF FROM JOB SCAMS

Educate yourself and read articles from government agencies, consumer protection and job search advice websites.

The Federal Trade Commission (FTC) is the nation's consumer protection agency. The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace.

- ❑ Consumer.gov
- ❑ Illinois: Office of State Attorney General
- ❑ Better Business Bureau
- ❑ AARP.org/Fraud Watch Network

HOW DO I SPOT A JOB SCAM?

According to Consumer.gov, What to Know and Do, scammers might:

- ❑ Promise you a job
- ❑ Promise you a government job
- ❑ Offer you "the secret" to getting a job
- ❑ Promise that you will make lots of money, especially by working at home
- ❑ Offer you a certificate to improve your chances of getting a job
- ❑ Charge you for their services -- especially in advance

workNet DuPage
americanjobcenter

HOW CAN I AVOID A JOB SCAM?

- ❑ Never deal with anyone who promises you a job. No one can promise you a job.
- ❑ Do not pay for information about a job.
- ❑ Even if there is a money-back guarantee.
- ❑ Do not deal with anyone who says you have to act fast.
- ❑ Ignore promises to make thousands of dollars working in your own home. Those promises are lies.

workNet DuPage
americanjobcenter

EVALUATING EMPLOYMENT/BUSINESS OPPORTUNITIES

- ❑Be wary of inflated claims of product effectiveness.
- ❑Be cautious of exaggerated claims of possible earnings or profits.
- ❑Beware when money is required up front for instructions or products.
- ❑Be leery when the job posting claims "no experience necessary".
- ❑Do not give your social security number when first interacting with your prospective employer.
- ❑Be cautious when dealing with individuals outside of your own country.
- ❑Be wary when replying to unsolicited emails for work-at-home employment.
- ❑Research the company to ensure they are authentic.
- ❑Contact the Better Business Bureau to determine the legitimacy of the company.

PROTECT YOURSELF FROM BOGUS JOB OFFERS

- ❑ Beware of unsolicited phone calls
- ❑ Beware of email and text communications
- ❑ Be careful of unsolicited emails from companies requesting personal financial information or asking you to interview remotely. You MUST research company.
- ❑ **If it looks too good to be true, it probably is!**

Begin forwarded message:

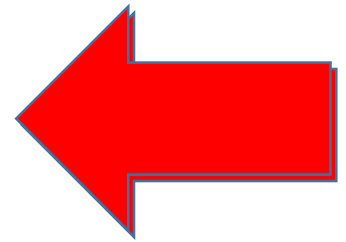
urgency

From: <info@corkwineandtapas.com>
Date: March 21, 2018 at 6:23:44 AM CDT
Subject: RE: CareerBuilder Job Application : Customer Service Representative/ Administrative Assistant / Front Desk Team Member

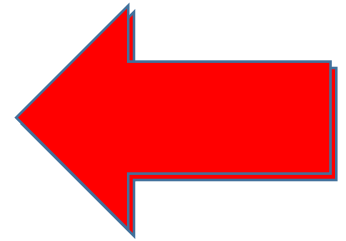
RED FLAGS

Job board

Dear Applicant,
I wish to inform you that Our recruitment team Has viewed your resume published on (careerbuilder.com) and we are pleased with your qualifications,we believe you have the required qualifications to undergo an online interview.



To proceed with this POSITION, you must undergo an online interview via Gmail Hangout. and You are required to have an account with gmail to enable you proceed.



I want you to setup a gmail Hangout (IM) if you don't have one and Instant Message (Ms Kimberly Rice) on her gmail ID via Hangout(hiringdesk2252@gmail.com) Asap for Your job briefing/ interview so that you can get Started for the position.

urgency

Interview schedule:
DATE: 03/21/ 2018
TIME: 10AM- 2PM EST

Grammar

Hope to read back from you as soon as possible.

Kind Regards.
HR Manager

USE VOICE MAIL:

A legitimate business or employer will leave a voice message with their contact info.

- ❑ **Google the phone numbers** to see if others have reported a scam –
  BEWARE: phone numbers look like they are coming from your area code or a legitimate business with caller id to make you think it is a real call.
  EXAMPLE: 630.333 – first three digits – could be a scam from out of the country.
  These are **spoofing calls**!
  Most always, scammers will not leave a message, they will move on to catch someone "Live".
  The more you answer these calls and interact, the more calls you will get.

- ❑ **IGNORE recorded robot voice mail messages**
  demanding immediate action & dire consequences.
- ❑ **Beware These Area Codes: 809, 284, 649 and 876**
  You could be calling back and getting huge charges on your phone bill. Each is for a Caribbean country, where the per-minute rate is higher than in the United States. The longer they keep you on the phone, the bigger your bill gets.

  Source: https://finance.yahoo.com/news/beware-area-codes-809-284-230616462.html

WHAT IF I ALREADY PAID SOMEONE BUT I DID NOT GET ANYTHING?

If you sent money and did not get help finding a job, report it to the Federal Trade Commission (FTC).

Call the FTC at 1-877-382-4357
Go online: www.ftc.gov/complaint

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

workNet DuPage
americanjobcenter

COVID-19 SCAMS

Fraud Alert

Office of Inspector General for the U.S. Department of Labor

UNEMPLOYMENT INSURANCE FRAUD ALERT

This is a Fraud Alert from the Office of Inspector General at the U.S. Department of Labor.

Fraudsters are perpetrating numerous schemes related to the COVID-19 pandemic. In one scheme, scammers have offered to help individuals file claims for unemployment benefits. The scammers then ask for personal information including social security numbers and dates of birth. The scammers may ask you to provide payment, or your credit card information, in assisting you in filing or qualifying for your unemployment benefits. You do not need to pay anyone to file or qualify for your benefits.

Unsolicited calls, social media platforms, and door-to-door visits are several ways that individuals have been targeted.

Be aware that your personal information may be used fraudulently without your permission.

Victims of these scams face potential harm. The personal information the scammers collect may be used to commit identity theft to file fraudulent unemployment insurance claims.

If you would like to report an allegation of fraud involving unemployment insurance or other U.S. Department of Labor activities or programs, please contact the OIG Hotline at: https://www.oig.dol.gov/hotline.htm or 202-693-6999 or 1-800-347-3756.

Government Agencies Will Not Call You To Demand Action Or Solicit Personal Information

Consumer Alerts

From the Federal Trade Commission

Avoiding Coronavirus stimulus payment scams

Scammers are using these stimulus payments to try to rip people off. They might try to get you to pay a fee to get your stimulus payment. Or they might try to convince you to give them your Social Security number, bank account, or government benefits debit card account number.

4 tips for avoiding a Coronavirus stimulus payment scam

Only use irs.gov/coronavirus to submit information to the IRS – and never in response to a call, text, or email.
The IRS won't contact you by phone, email, text message, or social media with information about your stimulus payment, or to ask you for your Social Security number, bank account, or government benefits debit card account number. Anyone who does is a scammer phishing for your information.

You don't have to pay to get your stimulus money.
The IRS won't tell you to deposit your stimulus check then send them money back because they paid you more than they owed you. That's a fake check scam.

Report scams to the Federal Trade Commission at ftc.gov/complaint.
To keep up with the latest scams, sign up for the FTC's consumer alerts.
(This post is part of the FTC's imposter scam series.)
Updated April 21, 2020

https://www.consumer.ftc.gov/blog/2020/04/coronavirus-stimulus-payment-scams-what-you-need-know

The Perfect Scam podcast
https://www.aarp.org/podcasts/the-perfect-scam/

AARP's weekly podcast *The Perfect Scam* profiles America's biggest scam stories. Hosted by Emmy award winning investigative journalist Michelle Kosinski, and leading fraud expert Frank Abagnale, the series introduces listeners to compelling personal stories from scam victims and their families. Interviews with professional con artists and leading experts in the topic to pull back the curtain on how scammers operate and share tips with listeners on how best to protect themselves.

AARP Fraud Watch Network Helpline: 877-908-3360

Monday through Friday, 7 a.m. to 11 p.m. ET

Report Scams and Fraud - free resource for AARP members and nonmembers alike

If you get a suspicious call, text or email (for example, requesting your bank account number, instructing you to buy a gift card or promising an expensive prize), or if you, a relative or a friend has given money or financial information to someone you now suspect was a scammer, call 877-908-3360.

In addition, your call helps AARP and our federal, state and community partners spot scam trends and respond to emerging threats.

AARP's Fraud Watch Network can help you spot and avoid scams. Sign up for free "watchdog alerts," review our scam-tracking map, or call our toll-free fraud helpline at 877-908-3360 if you or a loved one suspect you've been a victim.

Questions??

The short version is we need to be extremely cautious when opening emails, attachments and/or clicking on links.

Spotting a **phishing email** is becoming increasingly difficult, and many scams will even trick computer experts. However, there are some common signs to look out for:

- ❑ **Authority**
- ❑ **Urgency**
- ❑ **Emotion**
- ❑ **Scarcity**
- ❑ **Current events**

BE EXTRA cautious when opening emails, attachments or clicking on links.
Always hover your mouse over a link in an email to see where the link is taking you.

IMPOSTER scams info and Corona Virus/COVID-19

https://www.consumer.ftc.gov/taxonomy/term/864

FTC: Socially distancing from COVID-19 robocall scams

Scammers – and scammy companies – are using illegal robocalls to profit from coronavirus-related fears.

Coronavirus Outbreak Doesn't Slow Down Scammers

https://www.aarp.org/podcasts/take-on-today/info-2020/coronavirus-scams.html

The ***Consumer Financial Protection Bureau*** is a U.S. government agency that empowers you to take more control over your economic life and enforces federal consumer financial law.
Learn more about how the Bureau can help you.

Beware of scams related to the coronavirus

Recognize and prevent fraud and scams during the coronavirus pandemic.

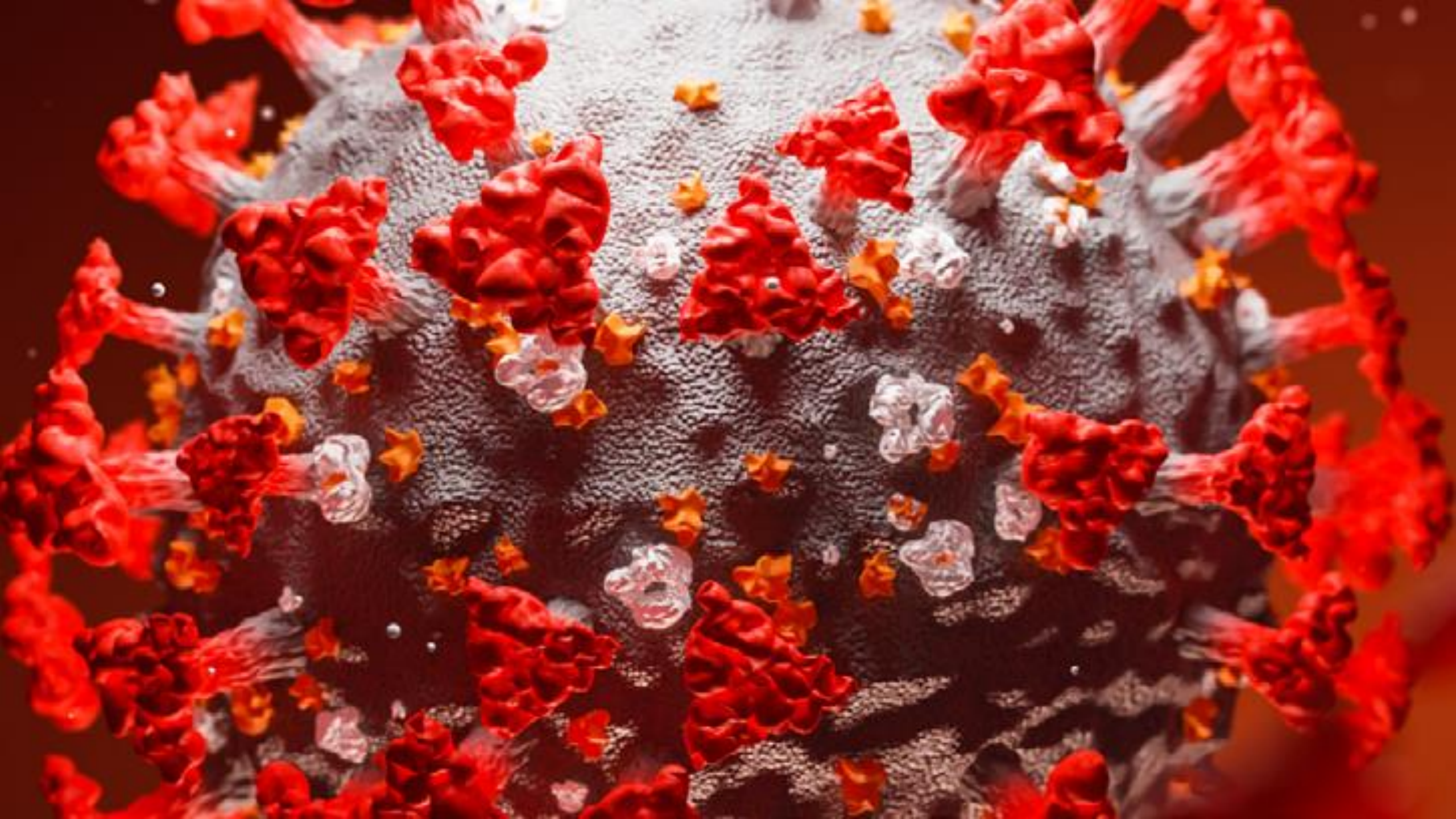
Learn more about protecting your finances during the coronavirus pandemic.

COVID -19 UI and Stimulus benefits

A short video from the Department of Labor has guidance on avoiding scammers and fraud related to COVID-19 and unemployment insurance

And while April 1st was **Census Day**, that doesn't mean it's too late to complete your questionnaire. In fact, it is required by law.

And as always, scammers are chasing headlines for their own personal financial benefit. One example — scammers hunting for personal info are calling folks just like you, claiming that completing the census is required in order to be eligible to receive coronavirus stimulus funds (the Census Bureau says stimulus fund distribution is NOT connected to completion of the census questionnaire). But census scams don't stop there.



Applicant Tracking Systems & Your Privacy

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Applicant Tracking Systems & Your Privacy

Human Resources/Talent Acquisition/Human Capital Management
must be aware of risks with handling job applicants' sensitive personal information.

Cybercriminals and hackers can use resumes, correspondence and data from prospective hires; companies can suffer financial and reputational loss and be prosecuted by federal regulators for failing to protect information.

"Personally Identifiable Information" or P.I.I. used in hiring process can include:

- Names/Addresses/SSN/DOB
- Background/Criminal/Credit checks
- Work History
- Emergency Contact Info

Applicant Tracking Systems & Your Privacy

Exposure Points:

- **Employer:** Websites/Email/Fax Machine/unsecured ATS (passwords/databases not encrypted)

- **Employer:** Interviews – often info passed through email and paper copies

- **Job Seeker:** Leaving email programs open on public computers or using unsecured public WIFI at libraries, coffee shops, restaurants, etc.


JobDiva
jobscience
TURBO RECRUIT
Octopus
people managing brilliantly, online
CIPHR
ALL ABOUT PEOPLE
BULLHORN
RESUMate
Affordable Recruiting Software
Bullhorn
JobDiva
icims
greenhouse
Lumesse
ORACLE
PEOPLESOFT
Deltek
HRsmart
jobscience
KRONOS
BIG BILLER
ClearCompany
PEOPLE MATTER
ApplicantStack
HYRELL
ADP
Taleo
PeopleStreme
Human Capital Management
empxtrack
Tracking Employee Excellence
Paycor
HealthcareSource
Quality Talent. Quality Care.™
AcquireTM
Talent Management
mindSCOPE
the applicantmanager
Cornerstone
ONDEMAND Empowering People
talentReef
JobAdder
CareerPlug
Jazz
Hireology
predicting success™
PeopleFluent
HiringThing
VidCruiter
vibe
HCM
cbs
DATIS
HUMAN CAPITAL MANAGEMENT
PAYROLL SOFTWARE SOLUTION
PeopleTrak
HR Software
PAYCHEX FLEX
ENTERPRISE

TOP SCAMS

2019 - States Most Vulnerable to Identity Theft & Fraud

https://youtu.be/-3yHXUGHlq4

Age seems to have a factor in both the susceptibility and dollars lost. For the younger consumers, aged 18 to 24, they have a susceptibility of 45.3% and a median dollar loss of $100.

Inversely, the opposite is true for consumers aged 65-plus, they have a susceptibility of 23.0% and an average dollar loss of $350.

As we look gender specific, men have a susceptibility of 35.5% and a median loss of $239 and women have a susceptibility of 35.7% with a median loss of $130.

Source: WalletHub

Riskiest scams of 2019: Employment Scams, Cryptocurrency Scams, Online Purchase Scams, Fake Check/Money Order Scams, and Advance Fee Loan Scams.

- ❑ 2019 riskiest scams for ages 18-54, students, and military spouses: Employment Scams
- ❑ 2019 riskiest scams for veterans and ages 65+: Travel/Vacation/Timeshare Scams
- ❑ 2019 riskiest scams for service members: Online Purchase Scams

- ❑ 2019 most impersonated organization: Social Security Administration

Top misperception: Contrary to widely held beliefs, younger consumers, rather than older adults, are most likely to have been scammed. Seniors, on the other hand, are more likely to lose more money.

Source: Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education & 2019 BBB Scam Tracker^{SM} Risk Report

2019's Top Job Scams - How the scam works

In 2019, job scams often impersonated Amazon. The reason why? Amazon was frequently in the news with its high-profile search for a second headquarters. In 2017, only 24 BBB Scam Tracker reports were employment scams that mentioned Amazon. In 2018, that jumped to 564.

Amazon scams and other employment cons typically follow the same patterns. Scammers contact victims by finding resumes posted online, posting phony job listings, or cold emailing targets. ***In most versions, the target starts corresponding with the "business" about a job opening. The pay is good, you can start immediately, and they don't even require an in-person interview! The catch of course is that job doesn't really exist.***

The scammer may

- ❑ ask you to pay upfront for training or a background check
- ❑ ask you to deposit a (fake) check and wire back part of the money
- ❑ get your bank account number to "direct deposit" your paycheck

How to Spot a Job Scam

- Be very cautious of any job that asks you to share personal information or pay money. Scammers will often use the guise of running a credit check, setting up direct deposit, or paying for training.
- If a job looks suspicious, search for it online. Google the title and company name. If the result comes up in many other cities with the exact same post, it may be a scam.
- Check out the business' website. Scammers often falsely use the names of real businesses. Check on the business's site or give them a call to confirm the position exists.

2017's Top Scams

1. **Phishing Emails/Texts – stealing money and information**
2. Can You Hear Me – Imposter phone scam
3. Online Purchase – fake websites
4. **Employment – job offer scams**
5. Tax Collection – fake IRS or Treasury Dept. calls/emails
6. Debt Collections – invoices, calls or emails for fake debts
7. Tech Support – calls, texts or emails from fake tech support agents
8. Sweepstake/Lottery/Prizes – fake claims to steal money upfront
9. Travel/Vacations – too good to be true offers
10. Identity Theft – fraudulent activity using your personal information

Source: BBB

2018's Top Scams

1. **Online Purchase** – fake websites
2. **Employment – job offer scams**
3. **Debt Collections** – invoices, calls or emails for fake debts
4. **Tech Support** – calls, texts or emails from fake tech support agents
5. **Tax Collection** – fake IRS or Treasury Dept. calls/emails
6. **Utility** – fake calls/emails claiming your service will be shut off unless you pay
7. **Fake Check/Money Order** – scammers send a fake check and convince recipients to send fees or the balance of an "overpayment" back
8. **Counterfeit Product** – often tied in with scam websites – consumers are sent cheap counterfeit items worth a fraction of the real item
9. **Phishing – a series of fake spoofed emails requesting money or personal information**
10. **Advance Fee Loan** – the promise of a "loan" – after you pay fees

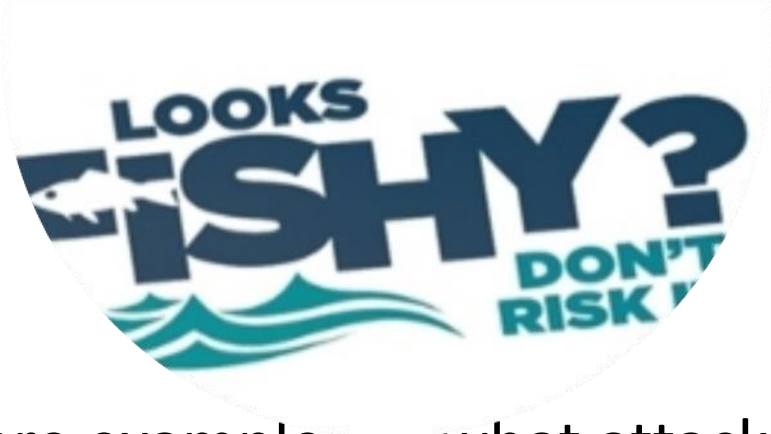
Six Scams to Be Wary of in 2020

A large portion of imposter scams are those pretending to be from the U.S. government. A few of the more common ones are:

- ❑ **IRS Scams**
- ❑ **Social Security Scams**
- ❑ **Telephone Scams**
- ❑ **Charity Scams**
- ❑ **Romance Scams**
- ❑ **Investment Scams**

SOURCE:https://www.usa.gov/features/six-scams-to-be-wary-of-in-2020

PHISHING EXAMPLES



The following messages are examples of what attackers may email or text when phishing for sensitive information:

- ***"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."***
- ***"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."***
- ***"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."***

To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit www.irs.gov/uac/report-phishing

A robocall is a phone call that uses a computerized autodialer to deliver a pre-recorded message, as if from a robot.

Keep your "scam antenna" up!

Being equipped with good information, you now have the advantage.

If it sounds too good to be true, it probably is.

The resources and information shared today will set you on the right path for a safe job search.

Pass it on!

According to the FBI, older Americans are frequent victims of Internet scammers because they have nest eggs and because of this:

They are less likely to report being swindled. Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed.

Email Format: joanjobseeker0915@gmail.com
Password is PASSWORD or 123456

Code for WDD Counselors

VIRTUAL JOB CLUB

workNet DuPage
americanjobcenter

Open for Registration Next Virtual Job Club :

May 15 **Staying Sane & Motivated During Times of Chaos** – Conor Cunneen

Future Virtual Job Clubs (Public):

- May 22 **Job Search: Research, Plan, Act** – Jim Fergle
- May 29 **How to Find a Federal Job** – Megan Straza
- June 5 **S.U.R.V.I.V.A.L. Guide for Job Search Wilderness –** Jim Fergle

Jim Fergle
www.worknetdupage.org
jfergle@worknetdupage.org

workNet DuPage
americanjobcenter

THANK YOU FOR ATTENDING JOB CLUB!

Resource Guide for Don't Get Slammed by Job Scams

workNet DuPage Career Center - Resources & Tips for Job Seekers and Employers

www.worknetdupage.org

Events/Calendar

Who's Hiring and much more!

workNet DuPage
americanjobcenter

ILLINOIS WORKNET
https://www.illinoisworknet.com/Qualify/Pages/SecurityAndPrivacy.aspx

ILLINOIS JOBLINK
https://illinoisjoblink.illinois.gov/ada/r/protect_yourself

The short version is we need to be extremely cautious when opening emails, attachments and/or clicking on links.

Spotting a **phishing email** is becoming increasingly difficult, and many scams will even trick computer experts. However, there are some common signs to look out for:

Authority - Is the sender claiming to be from someone official (like your bank, doctor, lawyer, government department)? Criminals often pretend to be important people or organizations to trick you into doing what they want.

Urgency - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.

Emotion - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

Scarcity - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Current events - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax time) to make their scam seem more relevant to you.
Your bank (or any other official source) should never ask you to supply personal information from an email. If you have any doubts about a message , call them directly. Don't use the numbers/emails in the email, but visit the official website instead.

BE EXTRA cautious when opening emails, attachments or clicking on links.
Always hover your mouse over a link in an email to see where the link is taking you.

ROBO CALLS

Robocalls are the No. 1 complaint from consumers to the FCC.
Video: https://youtu.be/PS3llQfRLD8

The Federal Communications Commission website contains information about services you can use to help block unwanted telemarketing calls, depending on what type of phone service you have and who your provider is: https://www.fcc.gov/unwanted-calls

The wireless industry (CTIA) also has extensive lists of call blocking apps that consumers download depending on what type of phone/operating system you have: http://www.ctia.org/consumer-tips/robocalls

Consumers can also contact the **Attorney General's Consumer Fraud Hotline: 1-800-386-5438** (Chicago).

"Census Day" may have just passed … but census scams are just beginning

How It Works

•Census scammers may contact you by phone, email, regular mail or home visit, or direct you to phony websites, seeking personal and financial information.

•Like other government impostors, they adopt the mantle of officialdom in hopes of winning your trust — and they have the added advantage of pretending to represent an agency specifically tasked with asking questions.

•Census scammers may threaten you with arrest if you fail to complete their questionnaire or provide them with the information they ask for.

What You Should Know

•All census mailings will have a return address of Jeffersonville, IN, the site of the National Processing Center. If it's from somewhere else, it's not from the U.S. Census Bureau.

•There are some things no genuine census survey or agent will ask for, whether by phone, email or in person — for example, your Social Security, credit card or bank account number. They won't ask for money. They won't threaten jail time if you don't answer their questions.

•Traditionally, those who do not complete their survey questionnaire could receive an in-person visit from a census representative. However, in light of the coronavirus pandemic, the U.S. Census Bureau has temporarily suspended in-person interviews.

•While taking part in the census is required by law, you CANNOT be imprisoned for failing to complete it.

What You Should Do

•Contact the Census Bureau's National Processing Center or the regional office for your state to verify that census communications you receive are genuine.

•Don't trust caller ID — scammers can use "spoofing" tools to make it appear they're calling from a real Census Bureau number. Call the National Processing Center at 800-523-3205, 800-642-0469 or 800-877-8339 (TDD/TTY) to verify that a phone survey is legitimate.

•You can report suspected scams to the regional Census Bureau office serving your state and to the Federal Trade Commission (online or at 877-382-4357).

Six Scams to Be Wary of in 2020

The most common, imposter scams, involve individuals pretending to be someone of trust to get money or personal information from a victim. This includes personal information like your Social Security number or access to your finances. The top frauds reported last year were from people pretending to be from the government, a well-known business, or a romantic interest in need of help.

A large portion of imposter scams are those pretending to be from the U.S. government. A few of the more common ones are:
IRS Scams: These scammers send a notice through email, mail, or phone calls in an attempt to gain access to your tax or banking information to steal your identity and money. Learn how to report these scammers if you've been affected.
Social Security Scams: Individuals pose as benefits investigators claiming a problem with your Social Security account. At times, they will tell you your number has been suspended and give a false number to call in order to "resolve" the issue. If you or a loved one has received one of these threatening calls, you can report them directly to the Social Security Administration.
Telephone Scams: Scammers try to steal money and personal information through phone calls, text messages or robocalls. They can convince you that you are getting free products or opportunities to invest your money or even get more. These fraudsters often make threats of jail or lawsuits if a fee isn't paid. Fight these by reporting them to the appropriate authorities.
Charity Scams: Charity scammers take advantage of disasters and tragedies by pretending to be legitimate. Imposters create fake organizations mimicking real ones to entice the generosity of those affected emotionally. Learn who to report them to.
Romance Scams: Finding love online can be a double-edged sword if you're not careful. It can be someone who lives near you or someone posing as a doctor or military officer stationed far away. Be aware that people can create fake profiles on dating and social media sites in an attempt to find a match and convince you to help financially.
Understand the signs of these situations and what to do if you've been affected by one.
Investment Scams: These scammers ask you to invest money to earn higher returns without financial risk. Companies then request you to bring more people in to do the same. They often need a constant flow of new people investing in order to make money. Ponzi and pyramid schemes are great examples of investment scams. Contact the Securities and Exchange Commission or your state's securities regulator to get help. SOURCE:https://www.usa.gov/features/six-scams-to-be-wary-of-in-2020