idwatchdog® from Equifax

Unemployment Benefits Fraud

What Employers Need to Know

According to the US Secret Service, there is currently a wave of unemployment fraud that is likely being executed by a well-organized crime ring and appears to have extensive records of individuals' personally identifiable information.[1] The number of incidents is staggering, according to reports,[2] and may be driving up the cost of taxes for businesses and causing frustration for both employers and workers.[3] Experts say that HR departments have a responsibility to respond quickly to these phony unemployment claims,[2] assist employees whose identity has been stolen, and alert employees to other common scams.[4]

In this paper, we will outline **key information** about:

- The current widespread unemployment benefits fraud
- How employers can better protect their organization against employment related scams
- How to help employees better protect themselves from identity theft

A Massive Wave of Unemployment Benefits Fraud Strikes the US

The FTC and other government agencies have warned that criminals, possibly based overseas, are filing claims for benefits, using the names and personal information of people who have not lost their jobs.[5] The scammers are targeting unsuspecting individuals—and employers—using stolen Social Security numbers and other personal details.[6]

Across a number of states,[2] both public and private employers have reported suspicious unemployment claims[6] filed in the name of current employees,[2] employees who retired or left the organization years ago, and even CEOs and senior-level management.[7] According to reports, scammers are attracted to the potential of a possible $10,000 to $20,000 payout per fraudulent claim.[8]

The Department of Labor's Office of the Inspector General estimated that pandemic-related unemployment scams totaled around $63B in losses through March 2021.[9]

idwatchdog® from Equifax

A Prime Target for Scammers

Experts say that unemployment programs have become a prime target for scammers because more funds are now available and some of the typical checks and balances for receiving benefits have been lifted.[7]

The federal government increased the weekly benefit amount through the Coronavirus Aid, Relief, and Economic Security Act (CARES Act).[2] It also offered unemployment benefits to workers who don't typically qualify, like the self-employed, freelancers, and part-timers.[8] Around the same time, many states lifted some or all of the standard unemployment qualifications, such as the one-week waiting period and the job-search requirement.[7] Further, fraudsters are exploiting overtaxed state unemployment agencies that are trying to process a massive amount of claims from an employment crisis unmatched since the Great Depression.[10]

Mobile banking apps and prepaid debit cards issued by some states may have also contributed to an increase in fraud.[9] New mobile payment methods may allow criminals to access financial accounts without appearing in person—or even risk being captured on an ATM camera—and debit cards can be easily moved on the black market by criminals looking to cash in on the funds.

How an Employee May Become an **Identity Theft Victim**

According to the FBI, scammers may get stolen identities[11] by:

- Purchasing information on the dark web
- Contacting victims impersonating government officials or trusted organizations
- Sending phishing emails
- Stealing electronic or physical data
- Data mining websites and social media

It's recommended that HR teams provide assistance and support to employees whose personal identifying information has been compromised.[2]

idwatchdog® from Equifax

What Employers Can Do if a Fraudulent Unemployment Claim Is Suspected

Employers often are the first to notice the fraud when they discover that a current employee or employees have been receiving unemployment benefits—sometimes for weeks.[7] The FTC advises employers to take steps to respond quickly to any suspicious unemployment claims and help support affected employees.[5]

- **Contact the appropriate state unemployment fraud hotline or website** - The Department of Labor (DOL) provides a list of unemployment fraud hotlines or websites by state.[12] The FTC suggests reporting the fraud online if possible, as it may save time and be easier for the agency to process.[5] (Most states offer an online option that can be found on the DOL's list.[12]) Depending on the state, the agency may request a fraud report from the employer, the employee, or both.[5]

- **Provide the employee a copy of the report** - The FTC advises that employers give employees a copy of any documentation of the report to the state, including any confirmation or case number.[5] Inform the employee if the state requires that they also report the fraud.

- **Provide support and resources to the employee for identity theft for their benefit—and yours** - Experts say that unemployment fraud can be the precursor to much larger issues related to identity theft.[13] A fraudulent unemployment claim is a sign that an employee's sensitive personal information is in the hands of criminals.[2] Employers should consider directing affected employees to file a report with the FTC at IdentityTheft.gov, notify the major credit bureaus, review their credit report, request fraud alerts or a credit freeze to help ensure that their personal information is not used to commit additional fraud.

- **Assist employees with identity theft protection for their benefit—and yours** - It's recommended that HR teams provide further assistance and support to employees whose personal identifying information has been compromised.[2] According to one study, survey respondents reported numerous workplace distractions due to identity theft, including having to take time off.[14] Twenty six percent of employers who responded to the survey currently offer identity theft protection as a benefit, and 70 percent would consider adding it to their employee benefits package.

- **Ensure there wasn't a company breach** - HR teams are advised to consult with their IT department[2] to confirm that databases containing employee information have not been compromised, especially if multiple employees report an issue.[7]

idwatchdog® from Equifax

How Employers Can Help Better Protect Their Employees' Personal Information Day-to-Day

Employers, by necessity, must collect and store sensitive employee data. With that data comes the responsibility for keeping it secure from internal and external threats. Learn these eight steps for helping better protect employees' personal information:

- **Conduct a risk assessment for employee personal identifying information (PII)** - According to experts, it's important to identify and understand where employee-related PII is collected, stored, and used within the organization.[7] With that understanding, HR and IT teams can work together to identify potential security weaknesses and resolve them before they are exploited by bad actors. It's recommended to ensure that written policies adequately cover the security of employee-related PII, which may be the largest source of PII maintained and used by the company.

- **Train employees on cybersecurity** - It's recommended that employers create a culture of security by implementing regular employee training as well as sending updates when new risks and vulnerabilities arise.[15] According to the FTC, topics that organizations should consider include email phishing scams,[16] ransomware attacks,[17] and business email imposter scams, in which the scammer sends an email that appears to come from another employee on the company's own network.[18] Employers are advised to notify employees about the increase in unemployment benefits scams[2] and ask them to report any suspicious claims to HR.[5]

- **Ensure strong physical security of documents and devices** - According to the FTC, lapses in physical security can expose sensitive company data to identity theft.[19] It advises that organizations store sensitive paper files in a locked cabinet or room and shred documents before disposal. It is recommended to secure all electronic devices using complex passwords, multi-factor authentication, and encryption.

- **Diligently review all unemployment claims** - According to experts, it is crucial for HR teams to diligently review[2] all unemployment claims or advise their third-party unemployment claims administrators to do the same. Experts say that HR should promptly review whether the named applicant for unemployment benefits is a current or former employee. A claim in the name of a current employee is likely fraudulent. If a claim is in the name of a former employee, HR should contact the individual to confirm whether the claim is legitimate.

- **Pay special attention to remote workers** - It's recommended that employers share tips with employees to help them maintain better security when working from home.[5] The FTC provides a list of online security tips for remote employees.[20] It's also advised that employers provide the tools and processes to help remote employees connect securely to company networks, such as a virtual private network (VPN).[7]

- **Consult with the IT department** - The FTC advises that organizations consider cybersecurity policies and practices related to other topics, such as vendor security and email authentication. It's advised to ensure that third-party vendors take steps to secure their own computers and networks.[21] Also consider email authentication technology, which can make it more difficult for scammers to send phishing emails that look like they originate from within the company.[22]

idwatchdog® from Equifax

- **Address data concerns in employee exit plans** It's advised that departing employees be given clear instructions that data and relevant equipment are property of the company.[23] Other suggestions include disabling or forwarding the individual's email, changing passwords to shared applications, and terminating virtual private network or remote access.

- **Communicate data breach response plans to all employees** - It's recommended that all employees know what to do if equipment, paper files, or data are lost or stolen, including whom to notify and what to do next.[19] The FTC provides Data Breach Response: A Guide for Business to help create a response plan.[24]

For more information on the impact of unemployment benefits fraud on victims and how employees can better protect themselves from identity theft and fraud, refer to the following **Employee's Guide**. It's designed to be shared with your workforce.

Sources Cited

1 The New York Times, "Feds Suspect Vast Fraud Network Is Targeting U.S. Unemployment Systems" (https://www.nytimes.com/2020/05/16/us/coronavirus-unemployment-fraud-secret-service-washington.html)

2 SHRM, The Society for Human Resource Management, "Unemployment Fraud Is on the Rise" (https://www.shrm.org/hr-today/news/hr-news/pages/unemployment-fraud-on-the-rise.aspx)

3 Montana Department of Labor & Industry, "Reporting Fraud and Identity Theft Online" (https://uid.dli.mt.gov/report-fraud)

4 SHRM, The Society for Human Resource Management, "HR and IT Should Team Up to Fight Cyberattacks" (https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/hr-it-fight-cyberattacks.aspx)

5 Federal Trade Commission, "Unemployment Benefits Fraud Puts Workers at Risk of More ID Theft" (https://www.ftc.gov/news-events/blogs/business-blog/2020/06/unemployment-benefits-fraud-puts-workers-risk-more-id-theft)

6 BenefitsPRO, "U.S. Unemployment Systems Are Under Attack, Secret Service Says" (https://www.benefitspro.com/2020/05/21/u-s-unemployment-systems-are-under-attack-secret-service-says/?slreturn=20210210121815)

7 SHRM, The Society for Human Resource Management, "Viewpoint: Fraudulent Unemployment Claims Are on the Rise" (https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/fraudulent-unemployment-claims.aspx)

8 CNBC, "Scammers Have Taken $36 Billion in Fraudulent Unemployment Payments from American Workers" (https://www.cnbc.com/2021/01/05/scammers-have-taken-36-billion-in-fraudulent-unemployment-payments-.html)

9 Chicago Tribune, "State unemployment systems face 'epidemic of fraud'; $63 billion paid out wrongly across US" (https://www.chicagotribune.com/business/ct-biz-unemployment-fraud-phony-claims-20210301-tcn4rvtcm5czzfq5uvnogrwuem-story.html)

10 The New York Times, "How Bad Is Unemployment? Literally Off the Charts" (https://www.nytimes.com/interactive/2020/05/08/business/economy/april-jobs-report.html)

11 FBI, "FBI Sees Spike in Fraudulent Unemployment Insurance Claims Filed Using Stolen Identities" (https://www.fbi.gov/news/pressrel/press-releases/fbi-sees-spike-in-fraudulent-unemployment-insurance-claims-filed-using-stolen-identities)

12 U.S. Department of Labor, "Report Unemployment Insurance Fraud" (https://www.dol.gov/agencies/eta/unemployment-insurance-payment-accuracy/report-unemployment-insurance-fraud)

13 Forbes, "Unemployment Benefits Fraud: What to Know and How to Protect Yourself" (https://www.forbes.com/sites/advisor/2020/10/09/unemployment-benefits-fraud-what-to-know-and-how-to-protect-yourself/?sh=1b85b0a332ff)

14 BenefitsPRO, "Legal, ID Theft Benefits Can Help Employees Stay on Track at Work" (https://www.benefitspro.com/2020/01/30/legal-id-theft-benefits-can-help-employees-stay-on-track-at-work/)

15 Federal Trade Commission, "Cybersecurity for Small Business: Cybersecurity Basics" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics)

16 Federal Trade Commission, "Cybersecurity for Small Business: Phishing" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing)

idwatchdog® from Equifax

[17] Federal Trade Commission, "Cybersecurity for Small Business: Ransomware" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware)

[18] Federal Trade Commission, "Cybersecurity for Small Business: Business Email Imposters" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/business)

[19] Federal Trade Commission, "Cybersecurity for Small Business: Physical Security" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/physical-security)

[20] Federal Trade Commission, "Online Security Tips for Working from Home" (https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-homel)

[21] Federal Trade Commission, "Cybersecurity for Small Business: Vendor Security" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/vendor-security)

[22] Federal Trade Commission, "Cybersecurity for Small Business: Email Authentication" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/email-authentication)

[23] Financial Management, "How to Prevent Employee Data Theft" (https://www.fm-magazine.com/news/2020/jan/how-to-prevent-employee-data-theft-21556.html)

[24] Federal Trade Commission, "Data Breach Resources" (https://www.ftc.gov/data-breach-resources)

An Employee's Guide to Unemployment Fraud and Better Identity Theft Protection

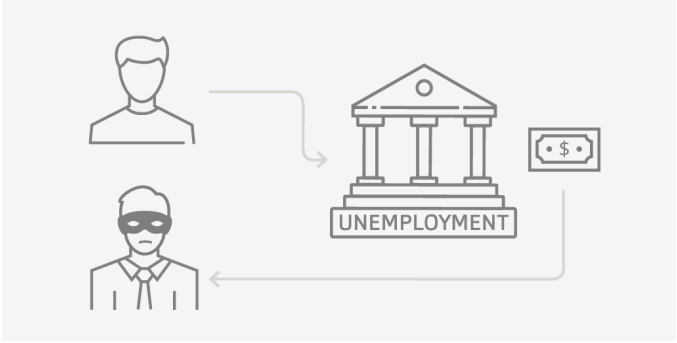
The Federal Trade Commission (FTC) has issued a warning that criminals may be using individuals' personal information, including Social Security numbers and dates of birth, to file fraudulent unemployment claims and collect phony benefits.[1] According to reports, this large-scale and sophisticated scam[2] is being conducted by a group of international fraudsters.

This employee's guide will outline key information about the current widespread unemployment scam, how to report it, and how individuals can help better protect themselves from identity theft and other fraud.

How the Unemployment Benefits Scam Works

Experts say that US unemployment programs have become a prime target for scammers because more funds are available during the pandemic and some of the typical checks and balances have been lifted.[3]

> **... this large-scale and sophisticated scam[2] is being conducted by a group of international fraudsters.**



The FBI states that these criminals use stolen identities to impersonate the victim and submit fake unemployment benefits claims on their behalf.[4] According to reports, scammers are attracted to the potential of a possible $10,000 or $20,000 payout per fraudulent claim.[5]

Scammers may get the stolen identities by purchasing information on the dark web, contacting victims impersonating government officials or trusted organizations, sending phishing emails, stealing electronic or physical data, or searching websites and social media.[4]

idwatchdog® from Equifax

Anyone Can Be a Victim

Most victims learn about an incident of unemployment benefits fraud from their employer or when they receive a notice from the state unemployment agency about an application for benefits filed using their identity.[1] By then, however, the benefits usually have been paid to an account the criminals control.

Other victims may not realize that they have been targeted until they try to file a claim for unemployment insurance benefits, receive a notification from the state unemployment insurance agency, receive an IRS Form 1099-G showing the benefits collected from unemployment insurance, or get notified by their employer that a claim has been filed while the victim is still employed.[4]

...victims may not realize that they have been targeted until they try to file a claim...

The **FBI advises** individuals to be aware of:[4]

- Communications regarding unemployment insurance when the individual has not applied for unemployment benefits
- Unauthorized transactions on bank or credit card statements related to unemployment benefits
- Any fees involved in filing or qualifying for unemployment insurance
- Unsolicited inquiries related to unemployment benefits
- Fictitious websites and social media pages mimicking those of government agencies

idwatchdog® from Equifax

The Impact of Unemployment Fraud on Victims

Though victims are not responsible for the stolen unemployment benefits, the fraud can lead to bigger concerns, which may include:

- **Slow replenishment of unemployment benefits** After an investigation confirms that an individual was in fact a victim of unemployment fraud, the victim's funds will be refilled, but it is a slow process that may take weeks or even months.[6] If the victim is employed, they will likely need to resolve the fraud and clear their name before they will be able to receive unemployment benefits in the future.[6]

- **Possible complications with the IRS** - Victims of unemployment fraud will likely receive a 1099-G tax form in order for the payments to be included as income on the victim's tax return.[7] Victims will not ultimately be held responsible for these taxes, but they will have to take action to resolve the issues. The IRS advises victims to contact their state for a corrected form showing that the amount of unemployment benefits they received was $0.[8] The IRS provides additional guidance for victims of this type of fraud.[8]

- **An increased risk of additional identity fraud** Unemployment fraud typically indicates that criminals have the victim's personal identifying information (PII), including Social Security number and date of birth. This puts the victim at risk for more identity theft and fraud,[1] such as new account fraud and tax identity theft. [9]

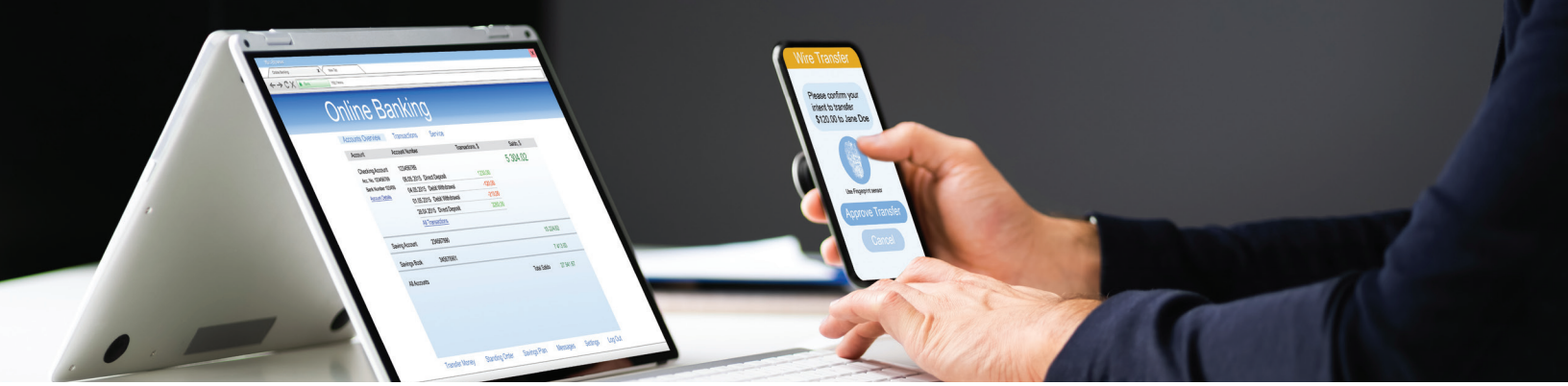
- **Unsuspecting victims could be lured as "money mules"** - In many cases, fraudulent unemployment payments are deposited into bank accounts controlled by the scammers.[10] However, if payments are sent to the victim's legitimate bank account instead, the criminals may continue the scam. Fraudsters may contact the victim by phone, email, or text message and impersonate an unemployment official, telling the victim that the payment was made in error in an attempt to get them to transfer the funds. This a money mule scam and participating in one could cause an individual more difficulties.[10]

What **Employees Can Do** If They Have Been a Victim of Unemployment Fraud

The FTC recommends the following steps if an individual suspects they have been the victim of unemployment benefits fraud.[10]

- Report the fraud to the employer
- Report the fraud to the state unemployment benefits agency - The Department of Labor provides a list of hotlines and websites by state.[11] The FTC recommends reporting the fraud online if possible, as it could save time and be easier for the agency to process. It's advised to keep any confirmation or case number and a copy of all communication.
- Report the fraud to the FTC at IdentityTheft.gov.
- Review credit reports regularly - The FTC advises checking credit reports every week for free through April 2022 at AnnualCreditReport.com.

idwatchdog® from Equifax



How Employees Can Better Protect Their Identity Day-to-Day

- **Set strong passwords** - The FTC advises individuals to create strong passwords for all devices and applications.[12] It is best to use passwords that are long, strong, and unique—at least 12 characters and a mix of numbers, symbols, and uppercase and lowercase letters. Some experts recommend using passphrases, which can help individuals create and remember more complex passwords.[13] Individuals should change their password if they are notified of a data breach by a company they do business with.[14]

- **Safeguard personal and financial information** - It's advised to be wary of any emails, calls, websites, text messages, or letters that request personal information, such as date of birth or Social Security number.[4] It's recommended not to carry a Social Security card in a wallet or purse and to only provide a Social Security number when absolutely necessary.[14]

- **Beware of phishing scams** - Phishing emails or text messages try to trick individuals into clicking a link or attachment that may infect the device with malware or lead to a cleverly disguised website to steal the user's information.[15] Phishing scams may appear to come from a known or trusted company, such as a bank, credit card company, social networking site, online payment website or app, or retailer.[16] Experts recommend that individuals carefully scrutinize the address of incoming emails, avoid clicking on suspicious links (such as those that don't begin with HTTPS or display the lock icon),[17] and use caution before opening attachments.[4]

- **Enable two-factor authentication when available** - Some accounts or apps offer multi-factor authentication, which is an extra layer of security that requires two or more credentials to log in, such as a unique passcode the user receives via text message.[16] Multi-factor authentication can make it harder for scammers to hack the victim's accounts, even if they have the username and password.

- **Monitor financial accounts** - The FBI recommends that individuals monitor their financial accounts on a regular basis and request a credit report at least once a year to look for any suspicious activity.[4] Immediately report unauthorized transactions to the financial institution or credit card provider. Credit reports can be ordered for free from Annualcreditreport.com.

- **Safely store devices and sensitive files** - It's recommended to keep laptops and other electronic devices locked and secure, and to never leave a device unattended, such as in a car or at a public charging station.[12] Consider keeping confidential information locked in a filing cabinet or room. Shred sensitive documents before putting them in the trash or recycling bin. It's best to collect mail every day and place a hold on mail during vacations or time away from home.[14]

idwatchdog® from Equifax

- **Secure home devices and networks** - The IRS advises using security software, including virus/malware protection and a firewall, and ensuring that they update automatically.[18] Consider enabling WPA2 or WPA3 encryption on home routers to help scramble information sent over the network, so outsiders can't read it.[12] If encryption is not available, it may be necessary to replace the router. It's also advised that individuals follow their employer's remote security practices, as for many people their home is now an extension of the office.

- **Use caution on public Wi-Fi networks** - The Department of Homeland Security advises individuals not to connect to unsecure public Wi-Fi networks, especially for confidential transactions, such as banking or online shopping.[19] It's advised to use a Virtual Private Network (VPN) or the user's own cell phone hotspot instead.[20]

- **Avoid becoming a money mule** - The FBI advises individuals to protect themselves by refusing to send or receive money on behalf of individuals and businesses for which they are not personally and professionally responsible,[21] and to be wary of online postings and messages promising easy money for little to no effort.[22]

- **Take appropriate action after a breach notification** The FTC provides a checklist for individuals whose information may have been exposed during a data breach.[23] Consider seeking professional help,[24] or contact the Federal Trade Commission for assistance.

- **Report suspected identity theft immediately** - If identity theft is suspected, immediately contact the three major credit bureaus to place a fraud alert and notify the FTC through its website Identitytheft.gov.

idwatchdog® from Equifax

Sources Cited

[1] Federal Trade Commission, "Unemployment Benefits Fraud Puts Workers at Risk of More ID Theft" (https://www.ftc.gov/news-events/blogs/business-blog/2020/06/unemployment-benefits-fraud-puts-workers-risk-more-id-theft)

[2] The New York Times, "Feds Suspect Vast Fraud Network Is Targeting U.S. Unemployment Systems" (https://www.nytimes.com/2020/05/16/us/coronavirus-unemployment-fraud-secret-service-washington.html)

[3] SHRM, The Society for Human Resource Management, "Viewpoint: Fraudulent Unemployment Claims Are on the Rise" (https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/fraudulent-unemployment-claims.aspx)

[4] FBI, "FBI Sees Spike in Fraudulent Unemployment Insurance Claims Filed Using Stolen Identities" (https://www.fbi.gov/news/pressrel/press-releases/fbi-sees-spike-in-fraudulent-unemployment-insurance-claims-filed-using-stolen-identities)

[5] CNBC, "Scammers Have Taken $36 Billion in Fraudulent Unemployment Payments from American Workers" (https://www.cnbc.com/2021/01/05/scammers-have-taken-36-billion-in-fraudulent-unemployment-payments-.html)

[6] Forbes, "Unemployment Benefits Fraud: What to Know and How to Protect Yourself" (https://www.forbes.com/sites/advisor/2020/10/09/unemployment-benefits-fraud-what-to-know-and-how-to-protect-yourself/?sh=1b85b0a332ff)

[7] Business Insider, "You Get a 1099-G Tax Form But Didn't Collect Unemployment in 2020, It Could Be Fraud. Here's What To Do" (https://www.businessinsider.com/personal-finance/unemployment-benefits-fraud-filing-taxes-1099-g-2021-1)

[8] Internal Revenue Service, "IRS Offers Guidance to Taxpayers on Identity Theft Involving Unemployment Benefits" (https://www.irs.gov/newsroom/irs-offers-guidance-to-taxpayers-on-identity-theft-involving-unemployment-benefits)

[9] ID Watchdog, "Beyond Financial Identity Theft: Learn About 6 Different Types" (https://www.idwatchdog.com/identity-theft-types)

[10] Federal Trade Commission, "Is a Scammer Getting Unemployment Benefits in Your Name?" (https://www.consumer.ftc.gov/blog/2020/06/scammer-getting-unemployment-benefits-your-name

[11] U.S. Department of Labor, "Report Unemployment Insurance Fraud" (https://www.dol.gov/agencies/eta/unemployment-insurance-payment-accuracy/report-unemployment-insurance-fraud)

[12] Federal Trade Commission, "Online Security Tips for Working from Home" (https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-homel)

[13] TechRepublic, "Replace Your Passwords with Passphrases: Here's How to Use Them to Remain Secure" (https://www.techrepublic.com/article/replace-your-passwords-with-passphrases-heres-how-to-use-them-to-remain-secure/)

[14] USA.gov, "Identity Theft" (https://www.usa.gov/identity-theft)

[15] WIRED, "How to Avoid Phishing Emails and Scams" (https://www.wired.com/2017/03/phishing-scams-fool-even-tech-nerds-heres-avoid/)

[16] Federal Trade Commission, "How to Recognize and Avoid Phishing Scams" (https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)

[17] PCMag, "How to Avoid Phishing Scams" (https://www.pcmag.com/how-to/how-to-avoid-phishing-scams)

[18] Internal Revenue Service, "Taxpayer Guide to Identity Theft" (https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft)

[19] CISA, U.S. Department of Homeland Security, "Holiday Online Shopping" (https://www.cisa.gov/sites/default/files/publications/19_1125_cisa_Holiday-Online-Shopping-Tip-Sheet.pdf)

[20] National Cybersecurity Alliance, "Online Shopping" (https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/)

[21] FBI, "Fraudsters Prey on Emotions and Bank Accounts in Money Mule Schemes" (https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fraudsters-prey-on-emotions-and-bank-accounts-in-money-mule-schemes)

[22] FBI, "COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic" (https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic)

[23] Federal Trade Commission, "When Information Is Lost or Exposed" (https://identitytheft.gov/databreach)

[24] The Washington Post, "Hackers Want Your Medical Records. Here's How to Keep Your Info From Them" (https://www.washingtonpost.com/national/health-science/hackers-want-your-medical-records-heres-how-to-keep-your-info-from-them/2018/12/14/4a9c9ab4-fc9c-11e8-ad40-cdfd0e0dd65a_story.html)

idwatchdog® from Equifax