HOW TO REPORT PHISHING-SCAMS-IDENTIFY THEFT – RECOVERY PLAN

This document will help with reporting phishing-scams-identity theft and communicating with membership in a culturally responsive way, and recovery plan development, as guided by Experian[1], Equifax[2], TransUnion[3], The U.S. Department of Health and Human Services[4], Office of Inspector General[5], and Federal Trade Commission[6].

Why It Matters:
Phishing-scams-identity theft can impact membership (people) in a negative influence on monetary assets but also cognitively and emotionally by building doubt every single time they are contacted via impersonation, phone calls, texts, or emails. AARP (2024) reports 21% of Americans (56 million U.S. adults) were defrauded out of 25.4 billion in telephone scams in 2023. With nearly 50 million people currently identified as disabled, a large percentage of American families are affected by crimes committed in fraudulent activity against persons with disability. For an individual, this shatters the reliability and validity of trusted relationships, organizations, systems, and communication modes. These schemes often exploit the vulnerabilities of people, limited English proficiency, racial and ethnic minority groups, such as their reliance and trust on assistance and support programs or their potential isolation from various social and learning opportunities to learn more about awareness-protective factors. Which means that as health and care providers, we must remain vigilant in bring this awareness of threat actors and education of fraudulent schemes to people, families, and communities we serve.

What is Phishing-Scams-identity theft:
Phishing-scams-identity theft is when scammers attempt to persuade people (victims) they need personal and protected information urgently, or the person (victim) will experience severe consequences, such as frozen accounts, personal injury, and-or loss of services-support programs.

Phishing	Scams
The fraudulent practice of sending emails or other messages intending to be from reputable companies-organizations to persuade a person to reveal personal-protected-identifiable information, such as passwords and credit card numbers.	A dishonest scheme, or fraudulent activity. Someone who makes monetary gain using illegal techniques, trickery to get personal-protected-identifiable information, such as financial, housing, and personal information.
Identity Theft	**Fraudulent Activity**
The fraudulent acquisition and use of a person's (victims) confidential-private identifying information, usually for financial gain. Is when someone uses personal information to open new accounts or make transactions in a person's (victims) name.	Is deliberate deceitful, dishonest, or untrue activity. Is about wrongful-criminal deception intended to result in financial or personal gain.
PHI: Protected Health Information	**PII: Personally Identifiable Information**
Is any information in the medical record or designated record set (date of birth, medical certificates, license information, vehicle registration details) that can be used to identify an individual and that was created, used, or disclosed while providing a health care service such as diagnosis or treatment.	Is any type of data that can be used to identify someone, from their name and address to their phone number, passport information, and Social Security numbers. This information is frequently a target for identity thieves, especially over the internet.

[1] "Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
[2] "Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
[3] "TransUnion. https://www.transunion.com/identity-protection
[4] "The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[5] "Office of Inspector General/SSA. https://oig.ssa.gov/scam-awareness/protect-yourself-from-identity-theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
[6] "Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

Universal Precautions-Culturally Responsive Care?
Practicing these universal precautions of fraudulent activity awareness, prevention, intervention factors compliment cultural humility and cultural competence, by increasing our cultural awareness and responsiveness-sensitivity to a person's cultural perspectives. And this connects to CLAS 1, 2, 4, 9, and 12. The National CLAS Standards are steps intended to advance health equity, improve quality/equality, and help eliminate health and care disparities.
CLAS 1: Provide effective, equitable, understandable, and respectful quality care and services that are responsive to diverse cultural health beliefs and practices, preferred languages, health literacy, and other communication needs.
CLAS 2: Advance and sustain organizational governance and leadership that promotes CLAS and health equity through policy, practices, and allocated resources.
CLAS 4: Educate and train governance, leadership, and workforce in culturally and linguistically appropriate policies and practices on an ongoing basis.
CLAS 9: Establish culturally and linguistically appropriate goals, policies, and management accountability, and infuse them throughout the organization's planning and operations.
CLAS 12: Conduct regular assessments of community health assets and needs and use the results to plan and implement services that respond to the cultural and linguistic diversity of populations in the service area.

Fraudulent activity and **cultural humility** – involve an ongoing process of self-exploration and self-critique combined with a willingness to learn from others. It means entering a relationship with another person with the intention of honoring their beliefs, customs, and values; **and this involves cross-culture interpretations of fraudulent activity.**

Fraudulent activity impact on **well-being (SDOH/HRSN):** Just over a quarter (26%) of fraudulent activity victims experienced physical changes as a direct result of losing money, including losing or gaining weight, experiencing headaches, and suffering from panic attacks. More than two-thirds (69%) said they experienced sleep problems.

Cultural impact of phishing, scams, and identity theft (*breaches ethical considerations*). Phishing, scams, and identity theft not only breach legal boundaries but also raises ethical concerns. It exploits trust, people, and communities, manipulates human behavior, and compromises individuals' privacy and security. Many people and members (victims) struggle with their mental and physical health. This type of fraudulent activity can be financially and emotionally devastating for some and increase the disadvantage, vulnerability, and inequality they suffer. Fraudulent activity can also cause lasting mental and physical trauma for victims and can result in lost opportunities for individuals and businesses.

Impact on suicide: scholars have identified that it is difficult to have solid data on fraudulent activity-driven suicide attempts, however by the time authorities get that data, it is often too late for many people and many families. It's never about the money. It's about the violation, the emotional distress, the real-life financial consequences, the disorientation. Often, it's also about lost love or friendship or dreams or trust — in others and in themselves.

[1] "Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
[2] "Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
[3] "TransUnion. https://www.transunion.com/identity-protection
[4] "The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[5] "Office of Inspector General/SSA. https://oig.ssa.gov/scam-awareness/protect-yourself-from-identity-theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
[6] "Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

HOW TO REPORT PHISHING-SCAMS-IDENTIFY THEFT – RECOVERY PLAN

arizona complete health

How to Report phishing-scams-identify theft?

Office of Inspector General (OIG) Hotline	Federal Trade Commission (FTC) Hotline
The OIG Hotline accepts tips and complaints from all sources about potentially fraudulent activity. They recommend submitting a complaint via the OIG Hotline online form. If the person prefers to contact the Hotline by phone, the telephone number is 1-800-447-8477. Be sure to include: • Date and time fraudulent activity. • Any other details from the fraudulent activity.	The Federal Trade Commission (FTC) works to prevent fraudulent, deceptive, and unfair practices. They also provide information to help consumers. The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. If you have been targeted by an illegal-fraudulent activity-practice or scam, report it. Be sure to include: • Date and time fraudulent activity. • Any other details from the fraudulent activity.
If a person is a victim of phishing-scams-identify theft, contact the HHS-OIG Hotline (1-800-447-8477) OIG Hotline online: https://oig.hhs.gov/fraud/report-fraud/	File a complaint with the Federal Trade Commission Hotline (1-877-382-4357) FTC Hotline online: https://reportfraud.ftc.gov/

Common signs of Exploitation:

1. The person says some money or property is missing.
2. The person is afraid or seems afraid of a relative, caregiver, or friend.
3. A person says a relative, caregiver, friend, or someone else keeps them from having visitors or phone calls, does not let the person speak for themself, or seems to be controlling their decisions.
4. Notice sudden changes in spending or savings. For example, a member and-or family is:
    a. Withdrawing money from accounts without explanation.
    b. Wiring large amounts of money.
    c. Using the ATM a lot.
    d. Not paying bills that are usually paid.
    e. Buying things or services they don't usually buy.
    f. Adding names on bank or other accounts that that they do not usually add.
    g. Not receiving account statements or bills.
    h. Giving new or unusual gifts to people.
    i. Changing beneficiaries of a will, advanced directives, power of attorney, life insurance policy, or retirement funds.
    j. Allowing a caregiver, friend, or relative to begin handling their money.
5. Skipping school, work, and-or health and care appointments.
6. Staying out late or overnight.
7. Unexplained gifts or new possessions.
8. Drug and alcohol misuse/abuse.
9. Secretive behavior-isolation.
10. Inappropriate or unsafe behavior.

[1] "Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
[2] "Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
[3] "TransUnion. https://www.transunion.com/identity-protection
[4] "The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[5] "Office of Inspector General/SSA. https://oig.ssa.gov/scam-awareness/protect-yourself-from-identity-theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
[6] "Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

HOW TO REPORT PHISHING-SCAMS-IDENTIFY THEFT – RECOVERY PLAN

Steps to Prevention-Intervention:

1. Contact your bank-financial institution immediately.
    a. Allow push alerts on mobile banking apps.
2. Contact major credit bureaus.
    a. Experian: 1-888-397-3742 www.experian.com
    b. Equifax: 1-800-525-6285 www.equifax.com
    c. TransUnion: 1-800-680-7289 www.transunion.com
3. Contact creditors (credit cards, utilities, cell providers)
4. Place a fraud alert or freeze on credit reports.
    a. Enroll in credit monitoring services.
5. Freeze telephone number when not in use.
6. Monitor accounts and close out old-unused accounts, or accounts that are believed to have been tampered with or opened fraudulently.
    a. Protect electronic devices.
7. Report any suspected identity theft to the Federal Trade Commission and-or Office of Inspector General.
8. File a report with local police department.
9. Do not answer calls with unfamiliar phone numbers (if it's important they will leave a message)
10. Do not open emails that not familiar with (perhaps call and verify the email from the sender before opening)
11. Don't rely on text messaging for account security codes.
12. Strengthen usernames and passwords to accounts.
13. Hide and secure personal and confidential information.
14. Keep contact information up to date.
15. Shred sensitive documents.

Do you need immediate mental health assistance?

- Call 1-844-53-4HOPE (4673) to reach the Arizona behavioral health crisis line, available 24/7/365 to any Arizona resident, even if you do not have health insurance coverage, or
- Call the 988 lifeline to be connected to a professional counselor 24/7/365, free of charge.

Phishing-Scams-Identity Theft Learning Resources:

- National Library of Medicine: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7235804/
- ACFE Insights: https://www.acfeinsights.com/acfe-insights/2023/7/24/protecting-the-disabled-community-from-fraudnbsp-nbsp#:~:text=Disabled%20individuals%20are%20often%20targeted,or%20even%20get%20medical%20services
- Provider*TRUST*: https://www.providertrust.com/blog/racial-disparities-in-healthcare-and-excluded-providers/
- Health Equity: https://www2.healthequity.com/protect
- RISE-HHS-OIG: Fraud alert: HHS-OIG telephone numbers used in spoofing scam (risehealth.org)
- Amazon: https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
- Arizona Attorney General: Fraud and Scams | Arizona Attorney General (azag.gov)
- AARP: Scam, Fraud Alerts - Protect Your Digital Identity (aarp.org)
- Pima County Attorney Fraud Unit: Fraud Department - Pima County Attorney's Office

[1] "Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
[2] "Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
[3] "TransUnion. https://www.transunion.com/identity-protection
[4] "The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[5] "Office of Inspector General/SSA. https://oig.ssa.gov/scam-awareness/protect-yourself-from-identity-theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
[6] "Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

NOTES:

[1] "Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
[2] "Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
[3] "TransUnion. https://www.transunion.com/identity-protection
[4] "The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
[5] "Office of Inspector General/SSA. https://oig.ssa.gov/scam-awareness/protect-yourself-from-identity-theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
[6] "Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data