Developmental Disabilities Administration

Phishing and Vishing

Care Provider Bulletin

May 2017

What is Phishing and Vishing?

- Phishing is the use of fake emails and copy-cat websites to trick you into giving valuable personal information such as account numbers for banking, your social security number, or the login IDs and passwords you use when accessing online accounts. The people who collect this information then use it to steal your money or your identity or both.
- Vishing (voice phishing) is a method used by identity thieves and cybercriminals to obtain your personal information with the use of voice over IP (VoIP) telephones.

Who is at Increased Risk?

- Individuals without computer skills
- Individuals who are not internet savvy
- Individuals who are more trusting of people they don't know

Examples of Phishing and Vishing Scams

- Emails stating that there was an unauthorized transaction on your account. To ensure that your account is not compromised, they ask you to click a link below and confirm your identity.
- Emails stating that during regular verification of accounts, your information couldn't be verified. They ask you to click on a link to update and verify your information.
- Phone calls stating that their records indicate that your account was overcharged, stating you must call within 7 days to receive your refund.
- Phone calls that have an automated message from someone claiming to be from the Internal Revenue Service (IRS). The caller threatens you with investigation and prosecution.
- A phone call from someone whose only goal is to get you to say the word "yes". They ask you if you can hear them, then record you saying yes. They then use that recording to claim that you agreed to something, and use that to make charges on your phone bill.

Did you Know?

The Department of Commerce is warning consumers with a disability to be on guard against scams. Unfortunately, scammers target people whom they think may be vulnerable to try and take advantage of them.

Common scams reported by consumers with a disability include fraudsters claiming:

- To represent a government authority or well-known business
- That they are looking for a relationship
- That the target has won a lottery or competition

Washington State
Department of Social
& Health Services
Transforming lives

Prevention

- Use trusted security software and set up automatic updates. In addition, use computer security practices from the Federal Trade Commission: https://www.consumer.ftc.gov/articles/0009-computer-security.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- Never believe that someone you don't know is going to give you money.
- Do not believe a person from another country who just needs you to "help transfer funds" and they need your bank account number to do so. Such scammers promise to give you a huge amount of money for helping them out. The result is an empty bank account.
- Sign up for scam alerts from the Washington State Attorney General's Office: http://www.atg.wa.gov/scam-alerts.

Vishing

- If you receive a suspicious or threatening phone call claiming to be from a reputable source, do not give them any information. Write down the number that appears on your caller ID, hang up, and report it.
- If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

Phishing

- Don't click on links in emails or attachments from unknown or untrusted sources. The links may take you to fake sites that look real.
- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text. Call the real company to let them know and see if something is needed.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information.
- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, such as a web address that begins with https (the "s" stands for secure). Also look for a closed padlock in the status bar.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.
- Visit the website of the Anti-Phishing Working Group at www.antiphishing.org for a list of current phishing attacks.

Always take extra precautions with personal information!

What to do if you've been a victim of Phishing or Vishing

- File a report with the Federal Trade Commission at www.ftc.gov/complaint
- If you receiving a phishing email pretending to be a company, tell the real company
- File a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center: www.ic3.gov
- Visit the Federal Trade Commission's Identity Theft website: www.consumer.ftc.gov/features/feature-0014-identity-theft

Sources & Resources

- **Federal Trade Commission,** https://www.consumer.ftc.gov/articles/0003-phishing
- **US Securities and Exchange Commission,** https://www.sec.gov/reportspubs/investor-publications/investorpubsphishing-htm.html
- **Washington State Office of the Attorney General,** http://www.atg.wa.gov/scam-alerts
- **Department of Commerce**, https://www.commerce.wa.gov.au/consumer-protection/scams-against-people-disabilities