IDAHO
DEPARTMENT OF FINANCE

BRAD LITTLE
Governor

PATRICIA R. PERKINS
Director

Contact: John Yaros
Securities Bureau Chief
Idaho Department of Finance
(208) 332-8000

NEWS RELEASE

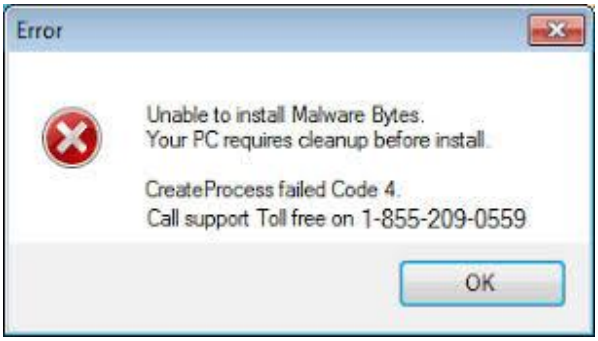
FOR IMMEDIATE RELEASE **April 9, 2025**

Financial Literacy Tip of the Week
Avoiding Tech Support Scams

Boise, Idaho- The growing use of digital technology is leading to an exponential increase in tech support scams that are leading to large financial losses for Idahoans. A tech support scam involves cybercriminals tricking unsuspecting victims into believing that their computer or electronic devices are either compromised by malware infections and viruses or potential system failures that require immediate maintenance when in fact no issues exist. Cybercriminals use these fake digital technology problems to fool victims into paying for services they do not need and/or to steal information that helps them perpetrate other crimes (e.g., identity fraud).

Financial losses from tech support scams are climbing, making it important for Idahoans to be vigilant. According to the FBI's 2023 Internet Crime Complaint Center (IC3), tech support scams were among the top five cybercrimes with **37,560 complaints** and a reported **$924.5M** in known losses. Over half of the complaints reported were from consumers over the age of 60. [1]

Common steps for a tech support scam include:



- **Initial Warning-** A potential victim receives a pop-up message, phone call, or text message that appears urgent and may use alarming language such as "Your Computer is at Risk!" or flashing lights to create panic.
- **Assistance Offer and Remote Access-** Cybercriminals offer to solve the problem and often either request remote access to a computer/electronic device or ask the

[1] https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

potential victim to download software.

- **Payment Request-** Once a victim accepts assistance, cybercriminals will either ask for payment via wire transfer, gift card, cryptocurrency, or credit card for fake services rendered for the purchase of unnecessary software that likely contains malware and viruses. Many times, these payment requests mention discount "emergency" rates.
- **Identity Theft-** If a cybercriminal gains access to a victim's computer or electronic device, they can potentially take over their financial accounts and/or steal other sensitive information including a victim's personal identifiable information (PII) for identity theft purposes.

It is imperative to apply the following best practices to protect against becoming a tech support scam victim:

- **Avoid Responding-** Never click on links, call phone numbers, or visit websites with prompts from pop-up messages claiming a computer or electronic device is compromised. If there is any doubt regarding a potential compromise, directly contact a legitimate entity through their formal channels.
- **Refuse Remote Access Requests-** Never give an unknown/unverified individual(s) remote access to your electronics if you did not initiate the contact originally.
- **Be Skeptical of Payment Demands-** If anyone creates a sense of urgency and demands payment to fix a technological issue that you did not initiate never send payment because it is almost definitely a scam.
- **Update Software and Use Anti-Virus Programs -** Use reliable anti-virus security software and immediately implement software updates/patches to identify and protect against potential vulnerabilities cybercriminals could exploit.
- **Identify Legitimate Technical Support -** Research and verify trusted technical support channels for companies and local repair shops both before and after an incident occurs.

If you fall victim to a tech support scam, it is important to immediately change your passwords, remove malware infections/viruses, contact your financial services companies, and report the incident to law enforcement and regulators. Specifically, any potential cybercrime incidents should be reported to the **Idaho Department of Finance, local law enforcement, the Federal Trade Commission (FTC), and IC3**. Reporting cybercrime enables key stakeholders to hold cybercriminals accountable, return victim funds/assets, and identify emerging trends.

****

Consumers can obtain information about financial firms, professionals, or products, as well as view more Department press releases and other information on the Internet at http://finance.idaho.gov or by contacting the Department at (208) 332-8000 or Idaho toll-free at 1-888-346-3378.