BE AWARE, VERIFY AND PROTECT: A GUIDE TO SCAM PREVENTION BASICS

Consumers are frequently targeted by scams intended to steal money and information. These scams appear in many forms and may impersonate legitimate companies and organizations to offer fake products and services. Fortunately, there are practical steps that consumers can take to stay alert and protect themselves — such as staying aware of the tactics criminals use, pausing to verify requests and safeguarding their devices and information.

1 BE AWARE OF TACTICS + **2** VERIFY REQUESTS + **3** PROTECT DEVICES & INFORMATION

STAY AWARE OF SCAM TACTICS

Awareness of common scams and red flags can help individuals identify suspicious messages or online offers and avoid financial losses by not responding to these unsolicited requests. Consumers who can identify a potential scam may be more likely to pause to verify a request before providing personal information or making a payment. For example, criminals may use spoofing — a tool that makes phone calls, emails and text messages appear to be from a known or trusted source — to impersonate banks and notify consumers of "fraud" affecting their accounts. Consumers who do not have an account with the financial institution may quickly identify the contact as a scam attempt. However, the scam message may seem more believable when consumers actually have accounts with a given financial institution. Ensuring customers know what distinguishes a legitimate message from their financial institution from a scam message, as well as encouraging them to pause to verify unsolicited requests, could prevent consumers from falling victim to a scam.

Some examples of resources that promote awareness of commons scams and red flags, such as urgency, threats of negative actions and too-good-to-be-true offers, include:

Federal Trade Commission email alerts: Stay Connected | Federal Trade Commission

Better Business Bureau Scam Tracker to report or look up a scam and sign up for scam alerts: Search for Scams | BBB Scam Tracker | Better Business Bureau

AARP Fraud Watch Network Scam-Tracking Map: Scam-Tracking Map: Find and Report Scams Near You

BE AWARE, VERIFY AND PROTECT: A GUIDE TO SCAM PREVENTION BASICS

VERIFY REQUESTS ARE LEGITIMATE

Taking the time to verify that a request or offer is legitimate can help prevent financial losses and the negative emotional impact often caused by scams. Some ways to verify the legitimacy of the request include:

- **Contacting the business** using trustworthy contact information from its official website, a monthly statement or other legitimate sources
- **Using a different communication channel** to verify the legitimacy of the request. For example, if the request was received via email, verify it by calling the requestor using a trusted phone number
- **Researching the request** or offer through independent sources, such as websites or the awareness resources listed above

When verifying a request, it is also important to remember that:

- Caller ID, email addresses and websites can be spoofed to appear legitimate. For example, a "1" or extra letter can be added to a legitimate email address so the new address can be used by criminals to send scam messages that appear to be from the legitimate sender. A minor change can be hard to spot if a person is not actively looking at it.
- Email accounts can be compromised and used by criminals to contact others for payment requests or account information change requests.
- Social media accounts that appear to belong to legitimate people also may be used to promote a scam opportunity, such as a "guaranteed" investment.
- Fake websites and applications for mobile devices can be created to mimic legitimate businesses and used to steal information or introduce malware.
    - Use a web browser with security tools that often can identify a scam website
    - Check for "https" in the website browser address to indicate the site is secure
    - Confirm that the URL web address does not contain misspellings or extra characters that could indicate the website is not legitimate
    - Close the website if there are any formatting issues, typos or links that do not work
    - Download mobile apps using the information posted on the legitimate company website, which may include the application name and link to download from a trusted app store

BE AWARE, VERIFY AND PROTECT: A GUIDE TO SCAM PREVENTION BASICS

PROACTIVE STEPS TO PROTECT AGAINST SCAMS

Safeguard Information

Along with awareness of scams, the following steps can prevent criminals from stealing money from individuals.

- Don't share personally identifiable information (e.g., name, address, Social Security number, date of birth) unless interacting with a legitimate and verified business, organization or agency.
- Provide only the specific information required to complete the request or transaction.
- Avoid sharing bank account details, including online banking login credentials. Use caution when posting information on social media sites that criminals could use to target and entice the user. For example, if a customer describes his dream vacation in an online post, criminals could use those details to send fake travel offers for that destination.
- Be aware of targeted ploys. For example, individuals looking for a new job may be contacted with fake job opportunities, often impersonating a known business to encourage responses.

Secure Devices and Accounts

Individuals should secure the devices they use to access sensitive accounts and personal information, move money and make online purchases.

- **Antivirus and anti-malware software** can help detect potential issues on devices. For example, clicking on links in phishing emails or posted on the internet can download viruses or malware. Criminals use viruses and malware to track user activity and capture keystrokes, which can include account usernames and passwords.
- **Multi-factor authentication (MFA)** is designed to prevent access to consumers' devices even if an unauthorized person obtains login credentials. Using an additional authentication factor, such as a one-time passcode or passkey, can prevent unauthorized access to accounts that could facilitate fraudulent payments.
- **Strong passwords** and not re-using passwords for multiple accounts makes it harder for criminals to gain unauthorized access.
- **Protect mobile devices** from account takeover, known as SIM swapping. (The SIM, or subscriber identity module, stores the information necessary for a smartphone to connect to a mobile network.) In this scam scenario, criminals attempt to impersonate an individual to have the phone number transferred to another device or "ported" to another carrier. Once criminals gain control of a mobile phone number, they can attempt to access online banking accounts, impersonate the customer and request one-time passcodes to approve payments. To prevent SIM swapping, discuss options with the mobile carrier to protect against SIM swapping and porting, such as setting up a required personal identification number (PIN) code to transfer a mobile phone number to another SIM card.

BE AWARE, VERIFY AND PROTECT: A GUIDE TO SCAM PREVENTION BASICS

Monitor Credit Profiles

Consumer access to credit, loans and employment often involves an individual's credit score. The score represents a financial and credit history and indicates whether a person is likely to repay the credit amount. It can impact the ability to obtain a loan and can influence the loan's interest rate. Businesses and organizations may use credit reports as part of background checks for new employees.

The following steps can help protect credit profiles and financial stability, such as:

- Request and review credit reports annually — at a minimum — to confirm the activity is valid or report any inconsistencies
- Work with the credit bureaus to address any unfamiliar accounts or credit inquiries
- Place a credit freeze with the credit bureaus to help prevent someone else from applying for credit
- Add a fraud alert on the credit file(s) to notify the legitimate person if there are any credit inquiries using this identity
- Explore credit monitoring services that can offer additional protection to alert consumers about their credit activity

BE AWARE, VERIFY AND PROTECT

Scam attempts will not stop, but individuals can take preventative steps to stop them.

- ***Be aware*** of scams and red flag indicators
- ***Verify*** requests directly with the legitimate entity prior to sending money or providing personal information
- ***Protect*** and safeguard devices and information

Taking these precautionary steps could help to prevent larger negative impacts of scams.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.