From: General Services Administration
Subject: Don't Take the Bait: Beware of Misleading Marketing, Imposters, and Phishing

Federal government agencies work to raise awareness about known online scams and fraudulent schemes that target government system users.

From time to time, GSA and IAE share information about common fraud schemes that target vendors registered in the System for Award Management (SAM). These scams attempt to use public information to defraud those interested in doing business with the federal government.

Just like users of any public online system, SAM.gov users with registered entities should always take caution to avoid getting caught up in a scam. Users might receive misleading marketing messages, fraudulent attempts to trick you out of money, or attempts to obtain your private information.

Third Party Companies and Misleading Marketing Practices:

There are some third-party companies that will offer to help register your entity in SAM.gov for a fee. **Registration in SAM.gov is always free**. While some users may find these services to be beneficial, please note that the GSA security policy strictly prohibits using another person's email address and password to access SAM.gov.

If you choose to pay a service to register or renew your entity you should be aware that any email or website that asks for money, no matter how official it looks, is not a government message or site. A source that leads you to believe that you must pay money to register in SAM.gov could be a fraudulent site. The government will never ask you to pay to register, update your registration, or renew.

Attempts to Trick You Out of Money:

SAM.gov users should always be on the lookout for fraudulent sources trying to get you to give them money without providing any service. While it's true that some companies provide registration services, scammers may offer a service they have no intention of providing. They may also pretend to be from a government agency requiring you to "pay a fee" by gift card, cryptocurrency, or wire transfer. The government will not ask you to pay fees using those methods. Again, you never need to pay to register, renew your registration, or "fix registration errors."

Phishing for Private Information:

Watch for attempts to get you to reveal personal information such as your SAM.gov password (phishing). Links in email messages can lead to look-alike pages that collect your login and go on to install malware or ransomware; have you "verify" more private data; or try to obtain access to your computer or network. Remember that your data in SAM.gov includes your bank account number; your Social Security Number or your Employer Identification Number; and employee names, email addresses, and phone numbers. Always be aware of bad actors trying to obtain this information.

How to be SAM.gov Smart:

Here are some ways to tell if an email or other source is trying to mislead you, defraud you, or get your private data:

- Check the sender's email address or the source's URL link. If they don't end with .gov, it's not from the government.
- Watch out for "tricky" links, especially ones that might end with gov.com or something else close to .gov.
- Don't answer requests to provide your information by phone or email. The government won't ever ask you to do that.
- Go to the website of the government agency the sender or caller says they represent. Look at the agency's practices and, if needed, contact the agency to verify the call or email.
- Verify any claims about registration errors or other problems by going to SAM.gov (not via an email link), signing in, and checking your registration yourself.
- If you're still not sure, you can contact our helpdesk at fsd.gov.

If you do want to use a service provider to manage your registration, it's a good idea to check the Better Business Bureau, independent references, or a search engine to confirm that you're working with a legitimate company before you pay anyone.

SAM.gov will never:

- Ask for personal information anywhere except within the SAM.gov system itself
- Ask for money or threaten legal action or liability
- Ask you to call or text anybody
- Send a link that doesn't end in .gov
- Advertise on social media

SAM.gov will send you several email reminders before your registration expires. We may also update you on the status of your registration or SAM.gov security issues. All of those emails will come from a .gov email address.

If you think you've received a fraudulent email or been the victim of fraud, ransomware, or another cyber crime, you can file a complaint with the Internet Crime Complaint Center (IC3). View the IC3 FAQs for more information about cyber crime and what's involved in filing a complaint.

You can report scams, fraud, and bad business practices to the Federal Trade Commission. Their FAQs have more information on what to include in your report.

Where can I find more information?

For more information about phishing and other potential scams targeting SAM.gov users, there are many articles on SAM.gov's help desk, the Federal Service Desk (FSD.gov), including:

- What should I do if I receive unsolicited contact from someone claiming to be a SAM.gov representative?
- How do I report suspicious activity with my record or user account in an IAE system?
- What can I do if I think I responded to a phishing email and attackers might have my information?