Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 15, 2021

Alert Number
I-101521-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Cyber Criminals Using Spoofed Unemployment Benefit Websites to Defraud US Public

The Federal Bureau of Investigation is issuing this announcement to alert and help the public recognize and avoid spoofed, or fake, unemployment benefit websites.

Cyber criminals have created these spoofed websites to collect personal and financial data from US victims. These spoofed websites imitate the appearance of and can be easily mistaken for legitimate websites offering unemployment benefits.

Cyber criminals register website domains and email addresses to appear like those which legitimately facilitate the processing of unemployment benefits. These domains and email addresses often will have misspelled words or will replace "[.]gov" with "[.]xyz." For example, one such domain is "illiform-gov[.]xyz." These domains lead victims to malign websites that are usually similar in appearance to legitimate counterparts. The fake websites prompt victims to enter sensitive personal and financial information. Cyber actors use this information to redirect unemployment benefits, harvest user credentials, collect personally identifiable information, and infect victim's devices with malware. In addition to a loss of benefits, victims of this activity can suffer a range of additional consequences, including ransomware infection and identity theft.

There were 385 identified domains hosted by the same IP address at 75.119.133.61, seven of which appear to impersonate government domains pertaining to unemployment benefits and are listed below.

Domain	Status
employ-nv[.]xyz	Active
employ-wiscon[.]xyz	Inactive
gov2go[.]xyz	Active
illiform-gov[.]xyz	Active
mary-landgov[.]xyz	Active
Marylandgov[.]xyz	Inactive
newstate-nm[.]xyz	Active
Newstatenm[.]xyz	Inactive

Tips on How to Protect Yourself:

- Verify the spelling of web addresses, websites, and email addresses to identify imitations.
- Look for a padlock icon next to the URL in the address bar to verify that the website you visit has a Secure Sockets Layer (SSL) certificate.
- Ensure operating systems and applications are updated to the most current versions.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Disable or remove unneeded software applications.
- Use strong two-factor authentication if possible, via biometrics, hardware tokens, or authentication apps.
- Do not open emails, attachments, or links from unknown individuals.
- Do not communicate with unsolicited text message/email senders by verifying the email header information.

Victim Reporting and Additional Information

If you believe that you have identified a spoofed unemployment benefit website:

- Contact your local law enforcement agency or your local FBI field office (contact information can be found at www.fbi.gov/contact-us/field-offices.)
- Immediately report the activity to the FBI's Internet Crime Complaint Center at www.ic3.gov.
- When reporting online scams, be as descriptive as possible in the complaint form by providing:
    - The website used by the actors.
    - Any information provided to/requested by the website.