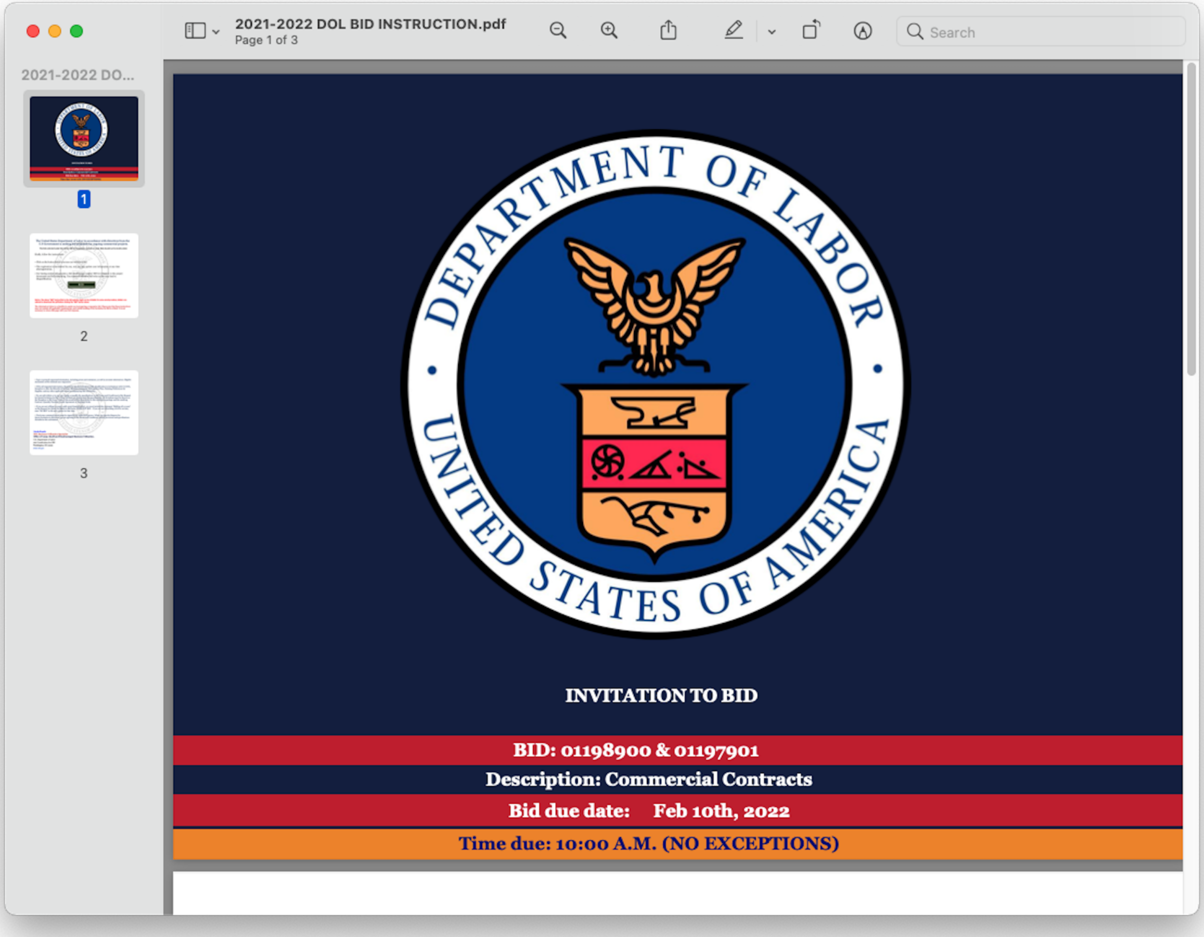
Fresh Phish: Phishers Lure Victims with Fake Invites to Bid on Nonexistent Federal Projects

inky.com/blog/fresh-phish-phishers-lure-victims-with-fake-invites-to-bid-on-nonexistent-federal-projects



INVITATION TO BID

BID: 01198900 & 01197901

Description: Commercial Contracts

Bid due date: Feb 10th, 2022

Time due: 10:00 A.M. (NO EXCEPTIONS)

Posted by Roger Kay

- Tweet
-

During the back half of 2021, INKY began detecting phishing emails that impersonated the United States Department of Labor (DoL). Eventually, the campaign grew to hundreds of instances.

INKY caught enough of these attempts to do a thorough analysis of the campaign, which is set out in this edition of Fresh Phish.

Quick Take: Attack Flow Overview

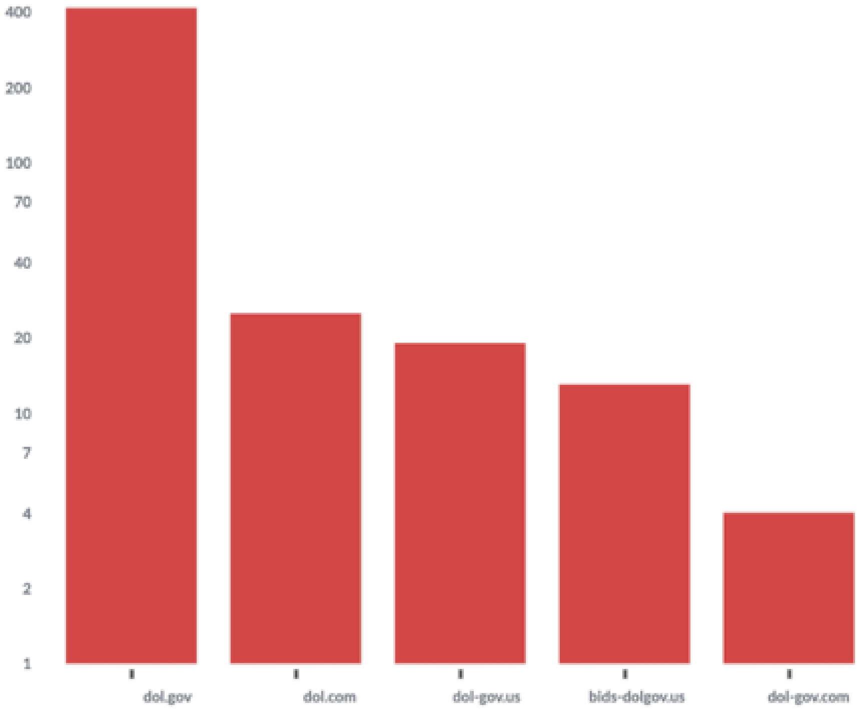
- **Type**: Phishing
- **Vector**: Spoofed DoL senders and newly created look-alike domains
- **Payload**: Malicious links in PDF attachments leading to credential harvesting sites
- **Techniques**: Brand impersonation, mail server abuse, VIP impersonation
- **Platform**: Google Workspace and Microsoft 365
- **Target**: Google Workspace and Microsoft 365 users

The Attack

In this campaign, the majority of phishing attempts had sender email addresses spoofed to look as if they came from no-reply@dol[.]gov, which is the real DoL site. A small subset was spoofed to look as if they came from no-reply@dol[.]com, which is, of course, not the real DoL domain.

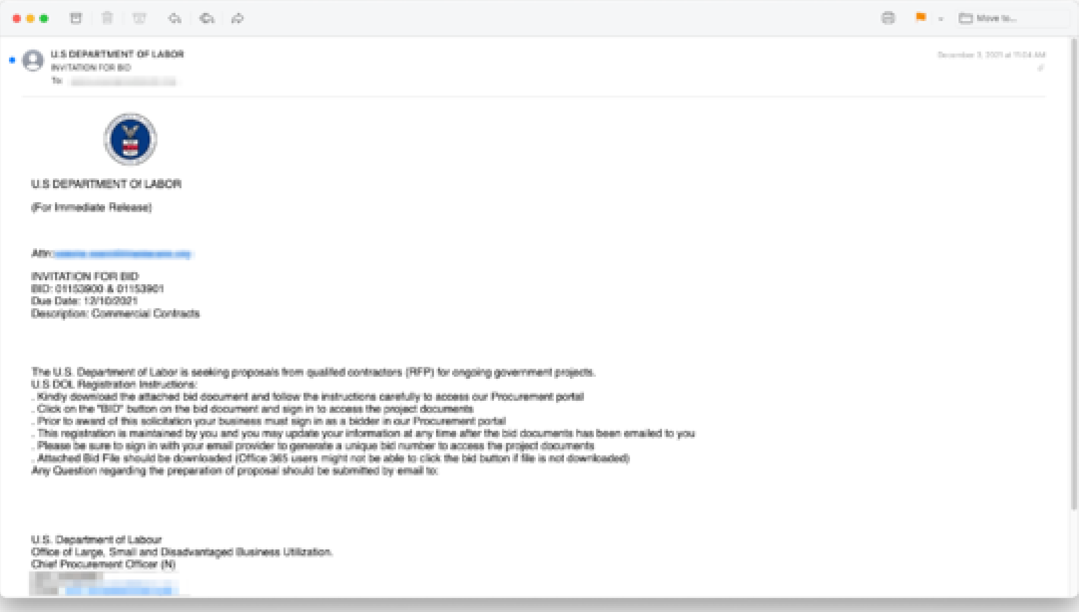
The rest came from a set of newly created look-alike domains:

- dol-gov[.]com
- dol-gov[.]us
- bids-dolgov[.]us



Distribution of spoofed domains

These phishing emails invited recipients to submit bids for “ongoing government projects" and claimed to be from a senior DoL employee responsible for procurement.



U.S DEPARTMENT OF LABOR
INVITATION FOR BID
To: [redacted]

December 3, 2021 at 11:04 AM

U.S DEPARTMENT OI LABOR

(For Immediate Release)

Attn:[redacted]

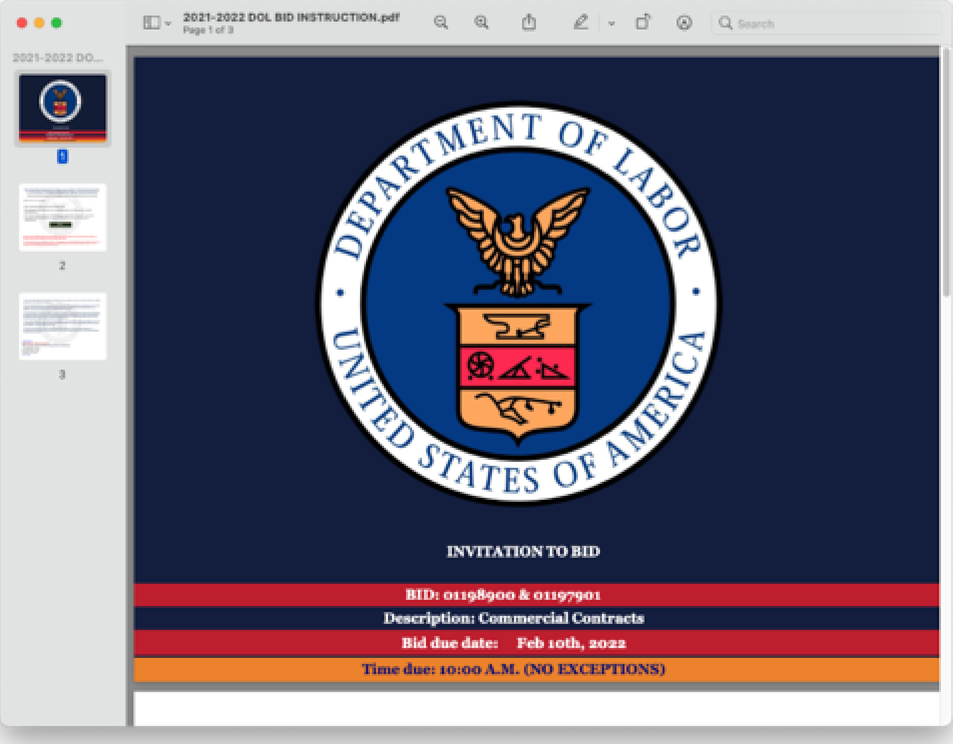
INVITATION FOR BID
BID: 01153900 & 01153901
Due Date: 12/10/2021
Description: Commercial Contracts

The U.S. Department of Labor is seeking proposals from qualified contractors (RFP) for ongoing government projects.
U.S DOL Registration Instructions:
. Kindly download the attached bid document and follow the instructions carefully to access our Procurement portal
. Click on the "BID" button on the bid document and sign in to access the project documents
. Prior to award of this solicitation your business must sign in as a bidder in our Procurement portal
. This registration is maintained by you and you may update your information at any time after the bid documents has been emailed to you
. Please be sure to sign in with your email provider to generate a unique bid number to access the project documents
. Attached Bid File should be downloaded (Office 365 users might not be able to click the bid button if file is not downloaded)
Any Question regarding the preparation of proposal should be submitted by email to:

U.S. Department of Labour
Office of Large, Small and Disadvantaged Business Utilization.
Chief Procurement Officer (N)
[redacted]

Email impersonating the U.S. DoL

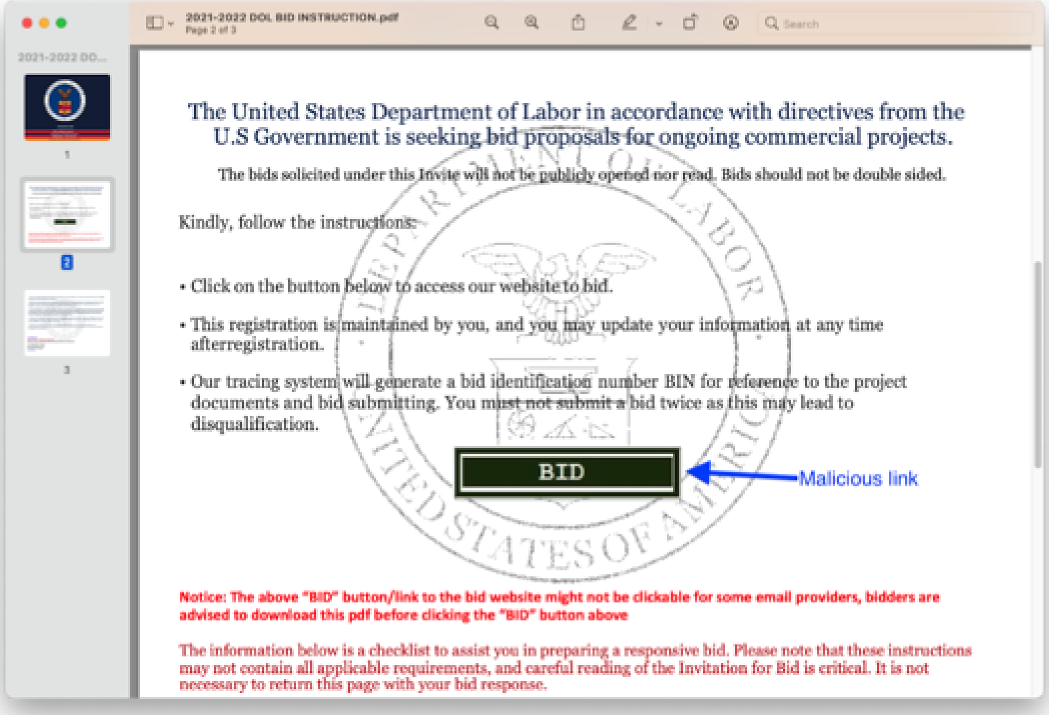
Each phishing email had a three-page PDF attachment (shown below) with well-crafted DoL branding elements.



INVITATION TO BID

BID: 01198900 & 01197901
Description: Commercial Contracts
Bid due date: Feb 10th, 2022
Time due: 10:00 A.M. (NO EXCEPTIONS)

Page 1 of PDF attachment



The United States Department of Labor in accordance with directives from the U.S Government is seeking bid proposals for ongoing commercial projects.

The bids solicited under this Invite will not be publicly opened nor read. Bids should not be double sided.

Kindly, follow the instructions:

- Click on the button below to access our website to bid.
- This registration is maintained by you, and you may update your information at any time afterregistration.
- Our tracing system will generate a bid identification number BIN for reference to the project documents and bid submitting. You must not submit a bid twice as this may lead to disqualification.

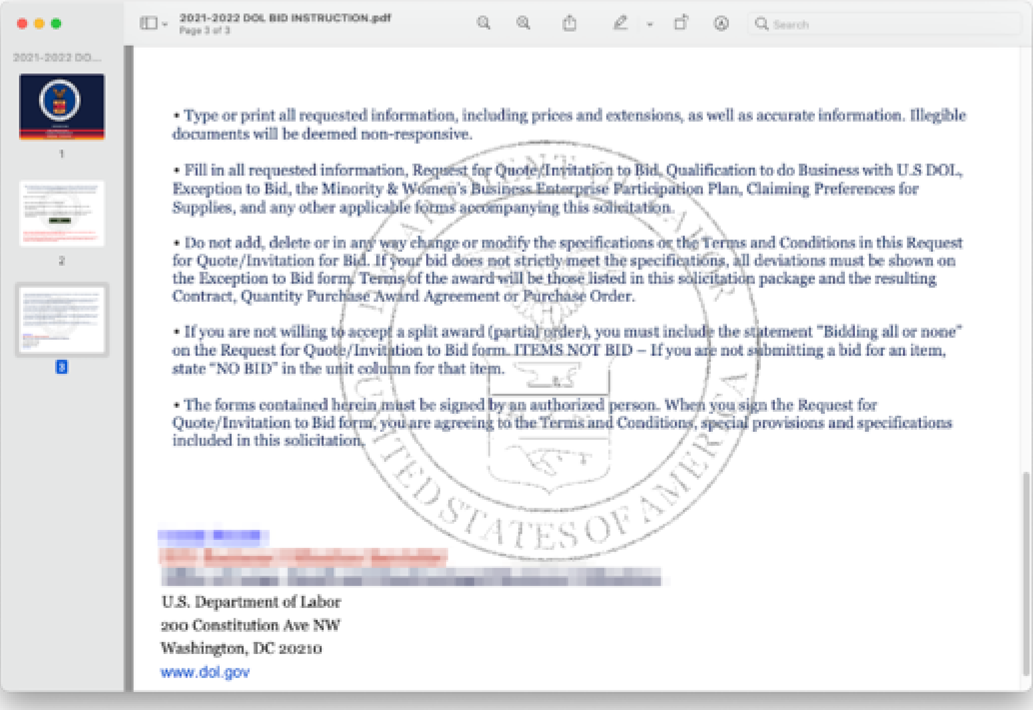
BID

Malicious link

Notice: The above "BID" button/link to the bid website might not be clickable for some email providers, bidders are advised to download this pdf before clicking the "BID" button above

The information below is a checklist to assist you in preparing a responsive bid. Please note that these instructions may not contain all applicable requirements, and careful reading of the Invitation for Bid is critical. It is not necessary to return this page with your bid response.

Page 2 of PDF attachment



- Type or print all requested information, including prices and extensions, as well as accurate information. Illegible documents will be deemed non-responsive.
- Fill in all requested information, Request for Quote/Invitation to Bid, Qualification to do Business with U.S DOL, Exception to Bid, the Minority & Women's Business Enterprise Participation Plan, Claiming Preferences for Supplies, and any other applicable forms accompanying this solicitation.
- Do not add, delete or in any way change or modify the specifications or the Terms and Conditions in this Request for Quote/Invitation for Bid. If your bid does not strictly meet the specifications, all deviations must be shown on the Exception to Bid form. Terms of the award will be those listed in this solicitation package and the resulting Contract, Quantity Purchase Award Agreement or Purchase Order.
- If you are not willing to accept a split award (partial order), you must include the statement "Bidding all or none" on the Request for Quote/Invitation to Bid form. ITEMS NOT BID – If you are not submitting a bid for an item, state "NO BID" in the unit column for that item.
- The forms contained herein must be signed by an authorized person. When you sign the Request for Quote/Invitation to Bid form, you are agreeing to the Terms and Conditions, special provisions and specifications included in this solicitation.

[redacted]

U.S. Department of Labor
200 Constitution Ave NW
Washington, DC 20210
www.dol.gov

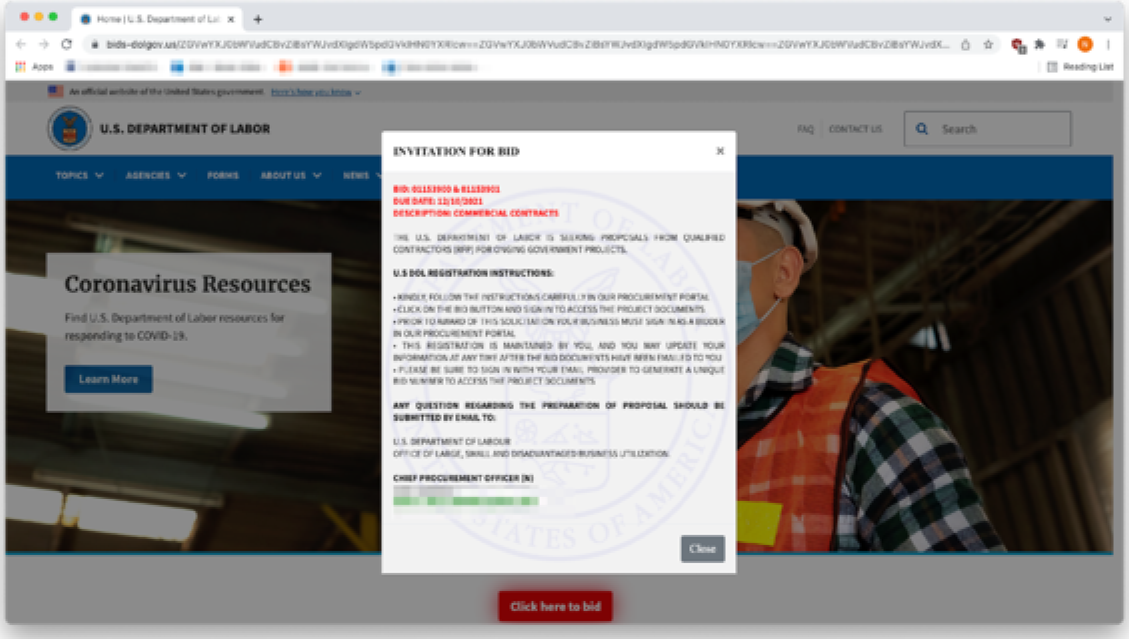
Page 3 of PDF attachment

Recipients were instructed to click the “BID” button on Page 2 to access DoL’s procurement portal. Behind the button was a malicious link. The links varied, but they all led to malicious domains that impersonated the DoL.

Here are the variants INKY detected:

- opendolbid[.]us
- usdol-gov[.]com
- bid-dolgov[.]us
- us-dolbids[.]us
- dol-bids[.]us
- openbids-dolgov[.]us
- open-biddolgov[.]us
- openbids-dolgov[.]com
- usdol-gov[.]us
- dolbids[.]com
- openbid-dolgov[.]us
- dol[.]global

What the victim saw when they reached the evil site was a set of fake instructions.



INVITATION FOR BID

BID: 01153900 & 01153901
DUE DATE: 12/10/2021
DESCRIPTION: COMMERCIAL CONTRACTS

THE U.S. DEPARTMENT OF LABOR IS SEEKING PROPOSALS FROM QUALIFIED CONTRACTORS (RFP) FOR ONGOING GOVERNMENT PROJECTS.

U.S DOL REGISTRATION INSTRUCTIONS:

- KINDLY FOLLOW THE INSTRUCTIONS CAREFULLY IN OUR PROCUREMENT PORTAL
- CLICK ON THE BID BUTTON AND SIGN IN TO ACCESS THE PROJECT DOCUMENTS.
- PRIOR TO AWARD OF THIS SOLICITATION YOUR BUSINESS MUST SIGN IN AS A BIDDER IN OUR PROCUREMENT PORTAL
- THIS REGISTRATION IS MAINTAINED BY YOU, AND YOU MAY UPDATE YOUR INFORMATION AT ANY TIME AFTER THE BID DOCUMENTS HAVE BEEN EMAILED TO YOU
- PLEASE BE SURE TO SIGN IN WITH YOUR EMAIL PROVIDER TO GENERATE A UNIQUE BID NUMBER TO ACCESS THE PROJECT DOCUMENTS

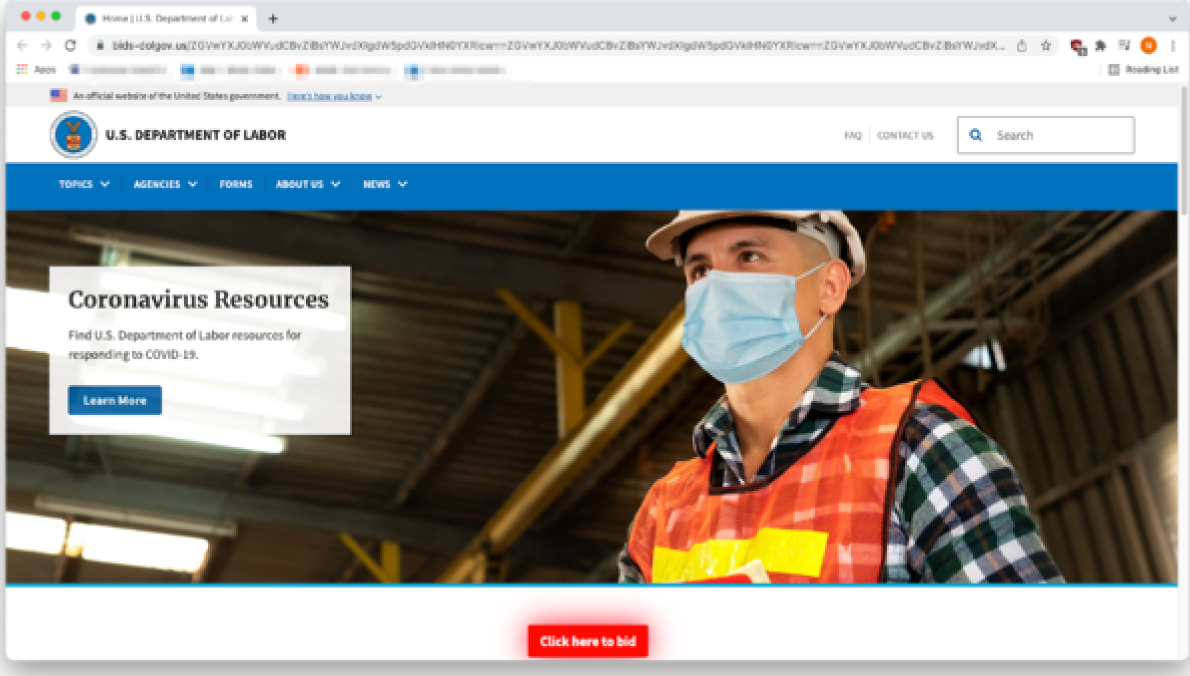
ANY QUESTION REGARDING THE PREPARATION OF PROPOSAL SHOULD BE SUBMITTED BY EMAIL TO:

U.S. DEPARTMENT OF LABOUR
OFFICE OF LARGE, SMALL AND DISADVANTAGED BUSINESS UTILIZATION

CHIEF PROCUREMENT OFFICER (N)
[redacted]

Fake instructions on how to submit a bid

When the victim closed the instructions, what they saw was an identical copy of the real DoL website. The clever phishers had simply copied HTML and CSS from the real site and pasted it into the phishing site.

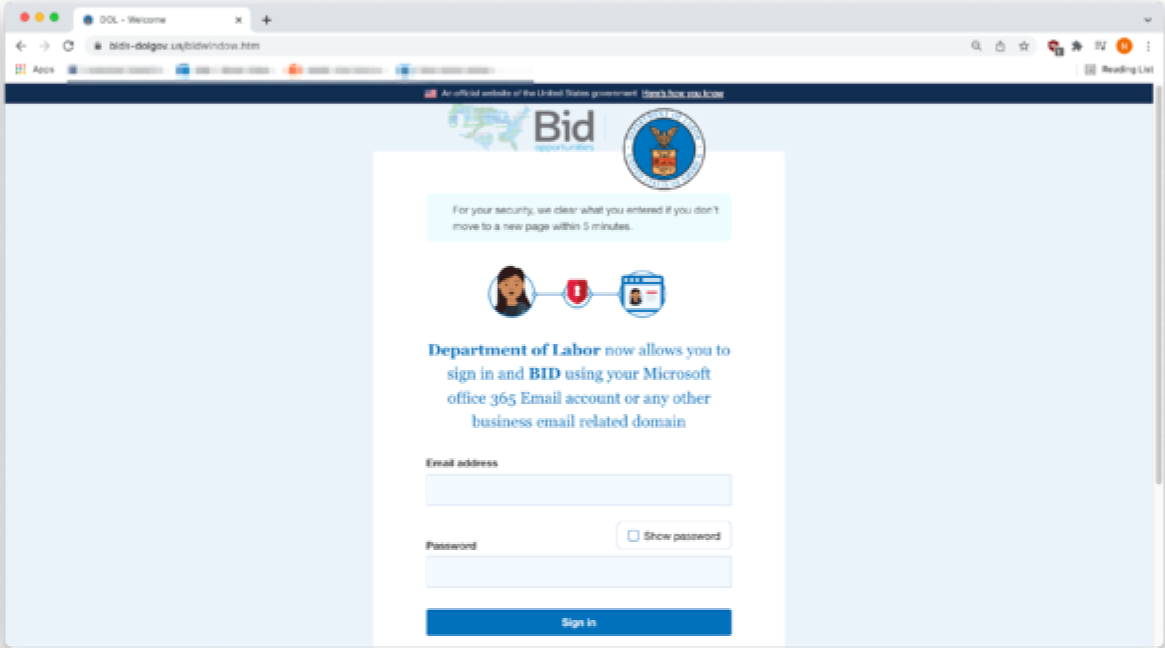

Home | U.S. Department of La
bids-dolgov.us/ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdX...
Apps
Reading List
An official website of the United States government. Here's how you know
U.S. DEPARTMENT OF LABOR
FAQ
CONTACT US
Search
TOPICS
AGENCIES
FORMS
ABOUT US
NEWS
Learn More
Click here to bid

Coronavirus Resources

Find U.S. Department of Labor resources for responding to COVID-19.

Identical copy of DoL site (except for red "Click here to bid" button)

Victims who clicked on the red "Click here to bid" button was presented with a credential harvesting form with instructions to sign in and bid using a Microsoft or other business email account.



DOL - Welcome
bids-dolgov.us/bidwindow.htm
Apps
Reading List
An official website of the United States government Here's how you know
Bid
opportunities

For your security, we clear what you entered if you don't move to a new page within 5 minutes.

Department of Labor now allows you to sign in and **BID** using your Microsoft office 365 Email account or any other business email related domain

Email address

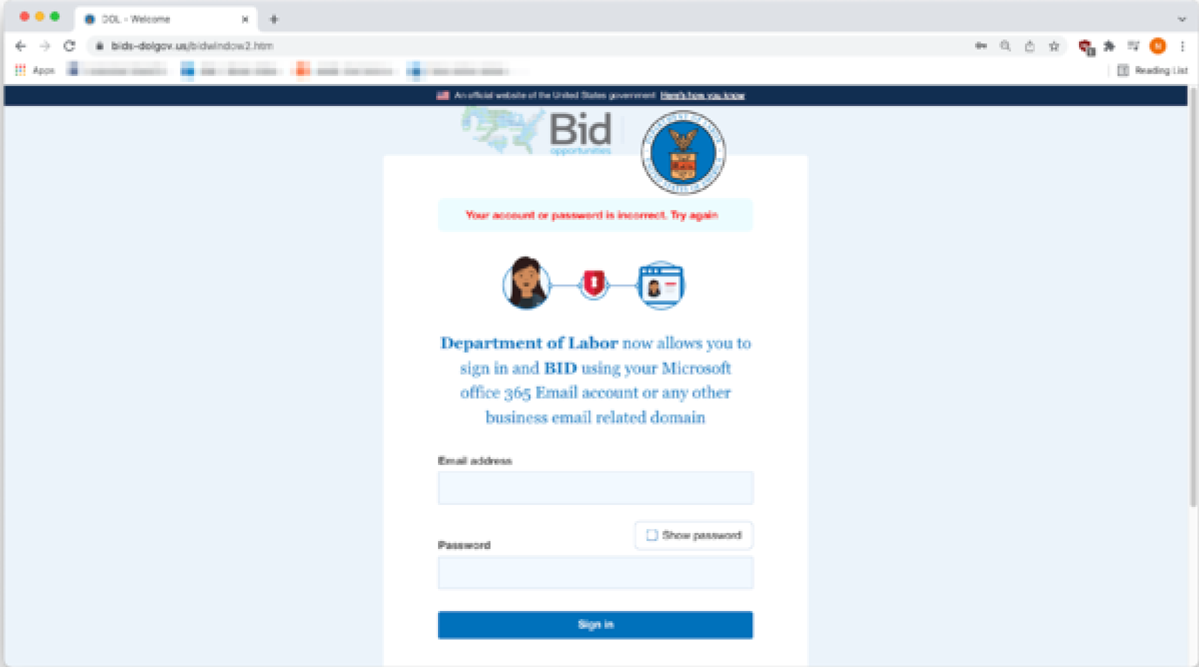
Password

□ Show password

Sign in

Credential harvesting form

When an INKY engineer made the first attempt at entering fake credentials, the site displayed a fake incorrect credentials error. But behind the scenes, those fake credentials had already been harvested (and either stored on the malicious site or emailed to the phisher).



DOL - Welcome
bids-dolgov.us/bidwindow2.htm
Apps
Reading List
An official website of the United States government Here's how you know
Bid
opportunities

Your account or password is incorrect. Try again

Department of Labor now allows you to sign in and **BID** using your Microsoft office 365 Email account or any other business email related domain

Email address

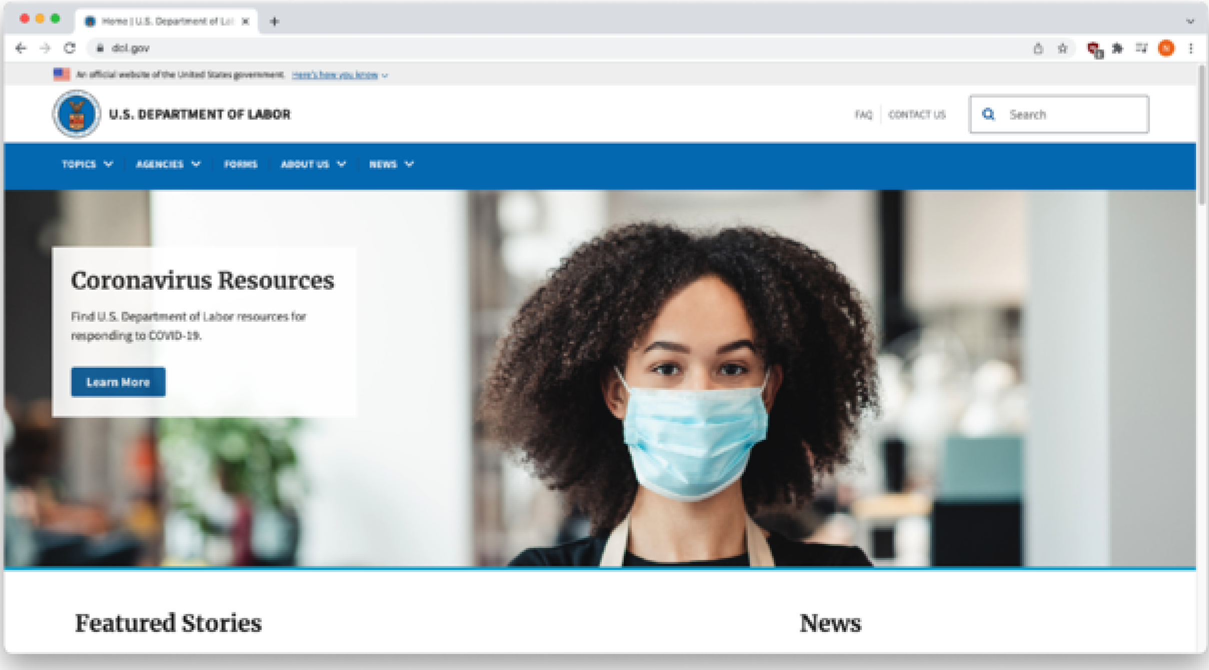
Password

□ Show password

Sign in

Fake incorrect credentials error

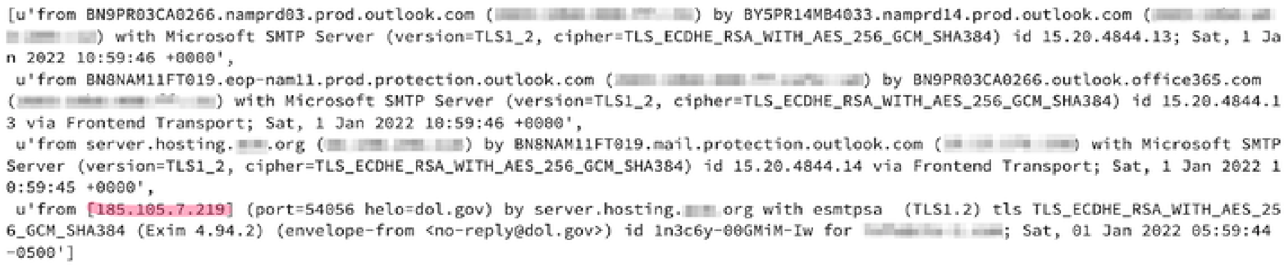
In a classic “blow-off,” when our engineer made a second attempt at entering fake credentials, they were redirected to the real DoL site. This nuanced touch, borrowed from con artistry that well predates the digital era, is designed to confuse the victim and delay the moment when they realize that they were taken.


Home | U.S. Department of La
dol.gov
An official website of the United States government. Here's how you know
U.S. DEPARTMENT OF LABOR
FAQ
CONTACT US
Search
TOPICS
AGENCIES
FORMS
ABOUT US
NEWS
Coronavirus Resources
Find U.S. Department of Labor resources for responding to COVID-19.
Learn More
Featured Stories
News

The real DoL site

Techniques

In the majority of these attacks (the ones in which the spoofed sender was either no-reply@dol[.]gov or no-reply@dol[.]com), the phishers were able to send their phishing emails from abused servers nominally controlled by a non-profit professional membership group.

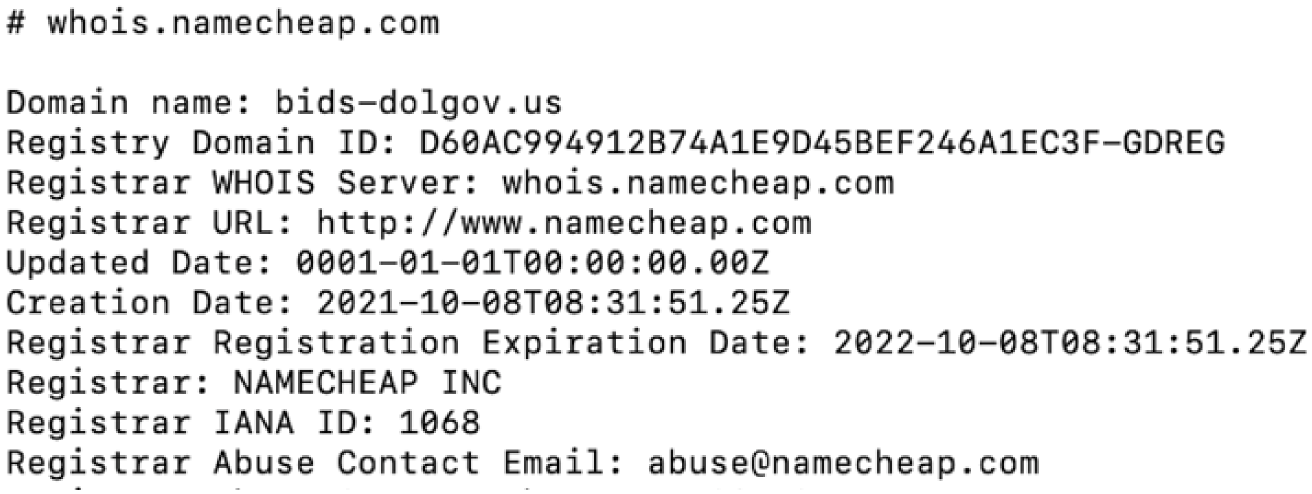


```
[u'from BN9PR03CA0266.namprd03.prod.outlook.com ([redacted]) by BY5PR14MB4033.namprd14.prod.outlook.com ([redacted]) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4844.13; Sat, 1 Jan 2022 10:59:46 +0000',
 u'from BN8NAM11FT019.eop-nam11.prod.protection.outlook.com ([redacted]) by BN9PR03CA0266.outlook.office365.com ([redacted]) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4844.13 via Frontend Transport; Sat, 1 Jan 2022 10:59:46 +0000',
 u'from server.hosting.[redacted].org ([redacted]) by BN8NAM11FT019.mail.protection.outlook.com ([redacted]) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4844.14 via Frontend Transport; Sat, 1 Jan 2022 10:59:45 +0000',
 u'from [185.105.7.219] (port=54056 helo=dol.gov) by server.hosting.[redacted].org with esmtpsa  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Exim 4.94.2) (envelope-from <no-reply@dol.gov>) id 1n3c6y-00GMiM-Iw for [redacted]; Sat, 01 Jan 2022 05:59:44 -0500']
```

Received headers of a phish sent on New Year's Day

In this example’s received headers (the path of servers through which the email travelled), the email originated from 185.105.7.219, and the non-profit’s abused mail server accepted it before passing it off to Microsoft Outlook servers. This technique allowed the phishing email to receive a DKIM pass for the reputable group’s domain. An investigation into 185.105.7.219 revealed that the IP address was associated with albacasino[.]com, a new domain created barely a week prior.

In other cases, the phishers used newly created domains to both send initial phishing emails and host fake DoL sites. Newly created domains are a black-hat favorite because they are able to pass standard email authentication (SPF, DKIM, and DMARC). Since they are brand new, the domains represent zero-day vulnerabilities; they have never been seen before and typically do not appear in threat intelligence feeds commonly referenced by legacy anti-phishing tools. Without a blemish, these sites used in this exploit did not look malicious.



```
# whois.namecheap.com

Domain name: bids-dolgov.us
Registry Domain ID: D60AC994912B74A1E9D45BEF246A1EC3F-GDREG
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2021-10-08T08:31:51.25Z
Registrar Registration Expiration Date: 2022-10-08T08:31:51.25Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
```

A WHOIS lookup surfaced a recently created phishing domain

Although several email security vendors use computer vision to detect impersonation sites, simplistic computer vision would not have helped in this case because the first thing the victim saw was the instructions, which concealed the actual impersonated site.

Recap of Techniques

- **Brand impersonation** — is done seamlessly by phishers who copy and paste HTML and CSS directly from the real DoL site to spoof it
- **Abuse of a mail server** — leverages a legitimate organization’s mail server to send phishing emails
- **Newly created domains** — are not yet known by threat intelligence feeds and therefore pass rudimentary security checks
- **Credential harvesting** — occurs when a victim tries to log into what they think is a real government site and ends up instead entering credentials into a form controlled by the phishers

Best Practices: Guidance and Recommendations

Official U.S. government domains usually end in .gov or .mil rather than .com or another suffix.

The U.S. government does not typically send out cold emails to solicit bids for projects.

Potential victims should be aware that it makes no sense to be asked to log in with email credentials to view a document on a completely different network.

For message administrators, it ought to be clear that SMTP servers should not be configured to accept and forward emails from non-local IP addresses to non-local mailboxes by unauthenticated and unauthorized users.

Read more of INKY's past Fresh Phish, and subscribe to receive our news and articles directly to your inbox.

INKY is an award-winning, cloud-based email security solution developed to proactively eliminate phishing emails and malware while simultaneously providing real-time assistance to employees handling suspicious emails so they can make safer decisions. INKY's patented technology incorporates sophisticated computer vision, machine learning models, social profiling, and stylometry algorithms to effectively sanitize emails, rewrite malicious links, detect and block security threats, mitigate sender impersonation, and more. Cost-effective and powerful, the INKY platform was developed for mobile-first IT organizations and works seamlessly on any device, operating system, and mail client. Learn more about INKY™ or request an online demonstration today.