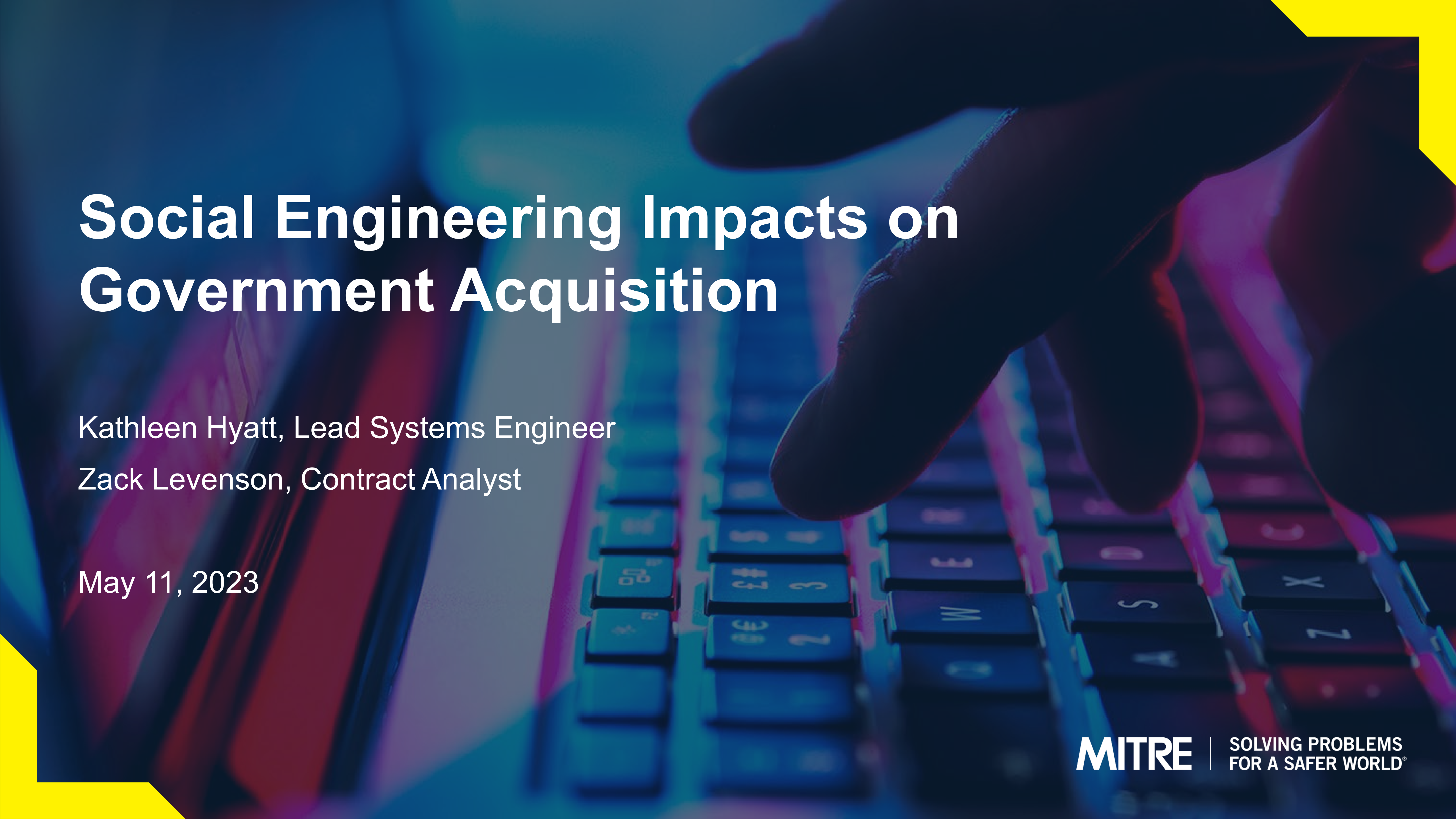


Social Engineering Impacts on Government Acquisition

Kathleen Hyatt, Lead Systems Engineer

Zack Levenson, Contract Analyst

May 11, 2023

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Research Question

Social engineering activities are becoming more prevalent as they rose 270% in 2021.

How do social engineering attacks directly affect the government acquisition community?

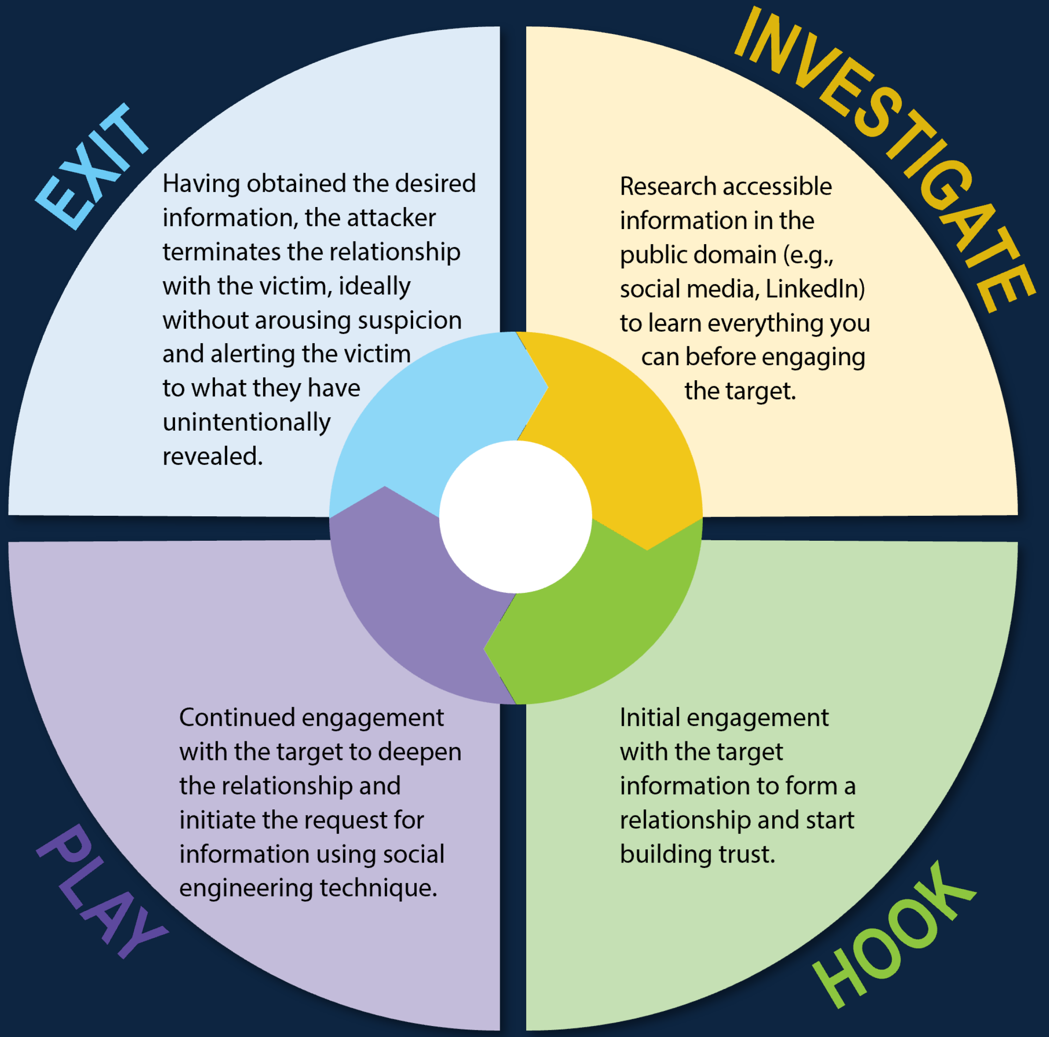
Methodology: Lifecycle of a Social Engineering Attack

Social Engineering

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

"Hacking the Human"

- Cognitive Exploitation
- Principles of Influence



INVESTIGATE: Research accessible information in the public domain (e.g., social media, LinkedIn) to learn everything you can before engaging the target.

HOOK: Initial engagement with the target information to form a relationship and start building trust.

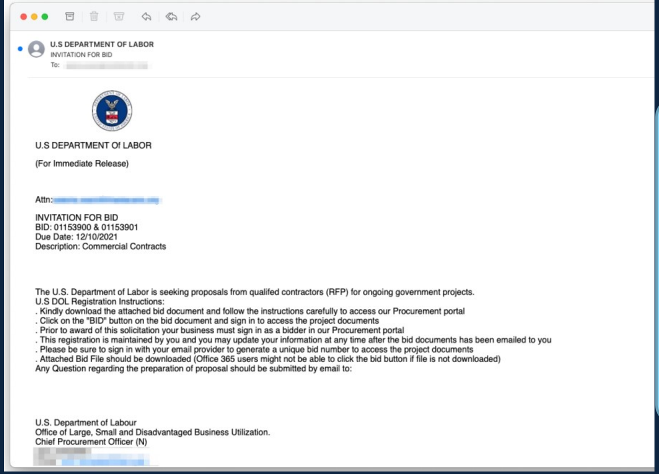
PLAY: Continued engagement with the target to deepen the relationship and initiate the request for information using social engineering technique.

EXIT: Having obtained the desired information, the attacker terminates the relationship with the victim, ideally without arousing suspicion and alerting the victim to what they have unintentionally revealed.

Figure represents a synthesized description of adversary behavior based on a collection of several previously published graphics detailing the attack cycle.

Operational Social Engineering: A Real-World Example

Phase 1: Investigation



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

U.S DEPARTMENT Of LABOR

(For Immediate Release)

Attn:[redacted]

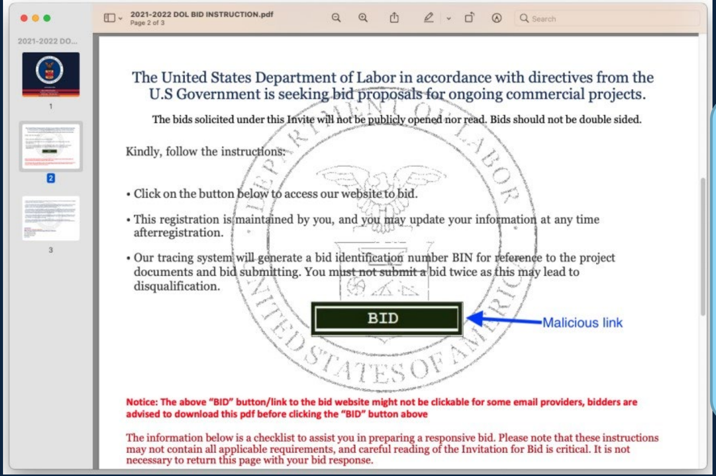
INVITATION FOR BID
BID: 01153900 & 01153901
Due Date: 12/10/2021
Description: Commercial Contracts

The U.S. Department of Labor is seeking proposals from qualifed 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 sent with invitation to submit bids. Looks genuine, but upon closer inspection, note the different spelling of “Labour” vs. “Labor”.

Phase 2: Hook



2021-2022 DOL BID INSTRUCTION.pdf
Page 2 of 3

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

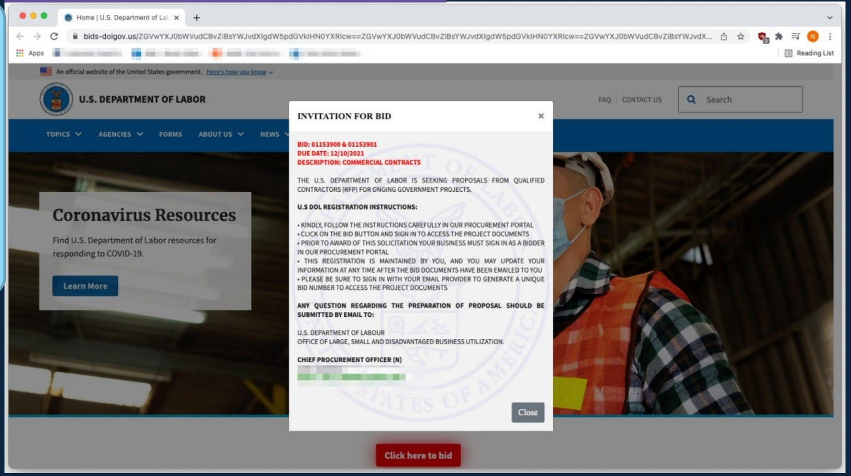
Malicious link

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.

Website where proposals are uploaded again looks genuine, however it contains a malicious link.

Phase 3: Play



Home | U.S. Department of Lab
bids-dolgov.us/ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdX...

An official website of the United States government. Here's how you know

U.S. DEPARTMENT OF LABOR

Coronavirus Resources

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

Learn More

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 ONGING 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.

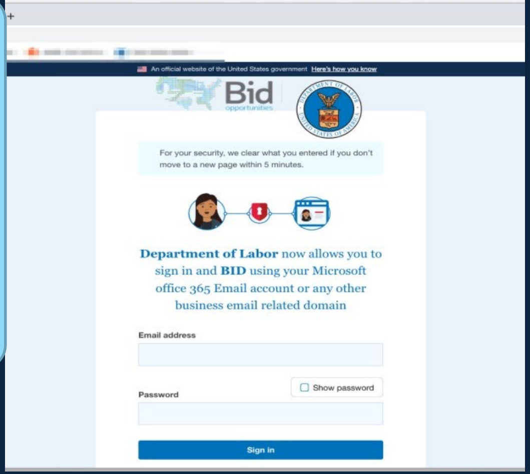
CHIEF PROCUREMENT OFFICER (N)
[redacted]

Close

Click here to bid

Link asks the user to enter credentials in order to submit the bid. The malicious link has now provided access.

Phase 4: Exit



An official website of the United States government Here's how you know

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

The final stage; the Attacker now has unlimited access. Once credential are inputted, directs to “true” DOL sites to the user’s MS 365 account and is provided

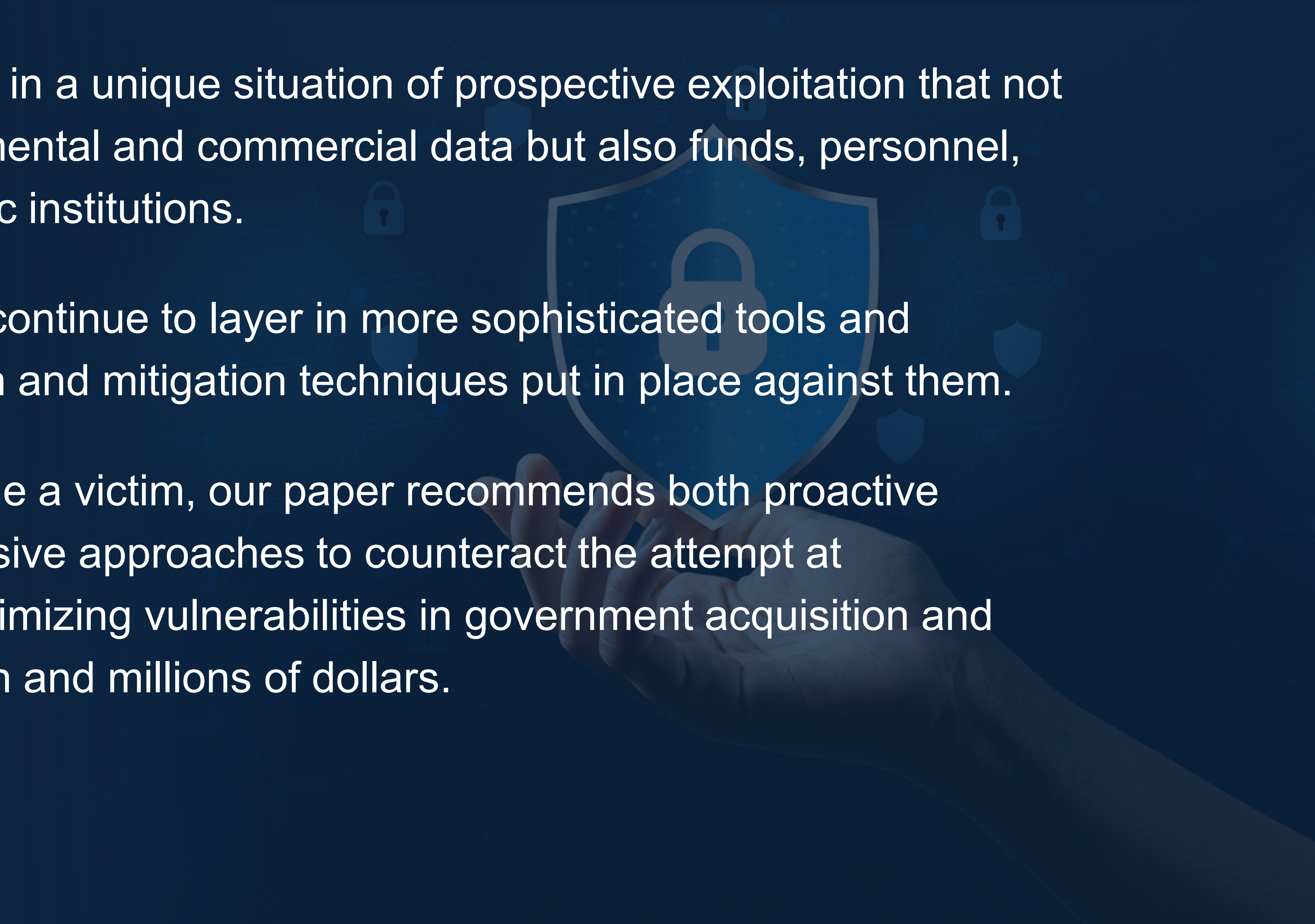
Impacts on Procurement from Social Engineering Attacks

- Due to the frequency with which the USG does business with and relies on contractors and industry, if a contractor is impacted by a social engineering attack, it may have an adverse effect on future government acquisitions and procurement processes as well as put missions in jeopardy.
- Disruptions to existing business relationships with contractors add to the overhead acquisition cost and make for a less efficient and more costly acquisition ecosystem.
- Other impacts include supply chain disruptions, price increases due to hacks, stolen information, and damages to reputation due to social engineering attack vulnerabilities.

Recommendations

- Defensive Factors and Vulnerabilities
  - Increased awareness of social engineering attacks through training
  - Considerations: Security skill level, Time in the work force, Internet usage
  - Focus on how to spot a social engineering attack
- Active Defense Measures and a Proactive Approach
  - Utilization of AI/ML tools
  - Reduce the attack service; i.e., analysis of what contract or acquisition activities can be done offline
  - Reduce staff task burden to avoid mistakes due to distraction

Conclusion



- Acquisition professionals are put in a unique situation of prospective exploitation that not only threatens sensitive governmental and commercial data but also funds, personnel, proprietary ideas, and democratic institutions.

- As social engineering attackers continue to layer in more sophisticated tools and tradecraft so must the prevention and mitigation techniques put in place against them.

- Knowing that anyone can become a victim, our paper recommends both proactive offensive approaches and defensive approaches to counteract the attempt at manipulation in the hopes of minimizing vulnerabilities in government acquisition and preventing the loss of information and millions of dollars.

We’d love to hear more about instances of social engineering attacks that you have encountered within your organizations. Please reach out to us!

Kathleen Hyatt

kbell@mitre.org

Zachary Levenson

zlevenson@mitre.org

https://www.linkedin.com/in/zack-levenson/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®