

MITRE study

Timeline / Messages

SEP 13: LinkedIn contact

Interest in your expertise at Stony Brook University

Hello Jan, I am a recruiter for a technical research and development firm with offices in the US and Beijing funded by the People's Republic of China. I hope you don't mind the direct approach, but we are currently looking for part-time consultants which I thought might be of interest given the high-quality experiences represented in your profile. We recently invested in projects that match your research and expertise at Stony Brook University, and we offer generous compensation for a variety of opportunities to collaborate. I would like to arrange a confidential conversation or meeting with you to give you an overview of our firm and available projects and answer any questions. Can you provide a phone number where I can call you?

Regards, Anna Anna Lei Recruiter at Illuminate HR

My answer:

Hi Anna, thank you for reaching out, but I am not interested at this time.

Timeline / Messages

SEP 22: LinkedIn contact

As anticipated, projects are starting at our Beijing office. I would hate to miss a chance to connect. In case you have concerns, I have been engaging with a well-regarded faculty member at Stony Brook, who has shared valuable presentations to our clients on unpublished, Department of Defense-funded research. These presentations have been extremely beneficial and well received. You will be privately well compensated for your time and information sharing. Regards, Anna

My answer:

I copied the message to my department chair and muted Anna.

Timeline / Messages

Sep 29: Email contact from Emily Pitek:

CC'd to Lawrence Zicarese <lawrence.zicarese@stonybrook.edu>

Subject: MITRE Research on Security Risks

Hello Jan,

I am a behavioral scientist with the MITRE Corporation, a not-for-profit organization that operates six Federally Funded Research and Development Centers (FFRDCs).
We are currently conducting a study to learn about research security risk in academia.

This study is trying to better understand the identification and reporting of research security risks in the academic research environment. The research security risks could be activities such as theft of ideas or data, unauthorized release of prepublication research, intentional damage/destruction of research-related resources, or intentional delay of research. Participant insights will help contribute to the development of research security approaches that are effective but frictionless, feasible, and support your university culture and values. **I am contacting you because you might have observed or experienced a situation recently involving a research security risk.** This could include observing or experiencing situations that are questionable in nature (e.g., possible access to pre-publication drafts or specific protocols/method prior to publication).

As part of our research effort, would you please be willing to participate in a 1-hour interview via Microsoft Teams or Zoom in the next week? This interview will help us gain contextual knowledge and insights about research security risk in the university research ecosystem. Your perspective is critical to help us advocate for university and researcher interests in possible security measures. Academia needs to develop targeted strategies to protect research while intentionally maintaining the open and collaborative environment needed for innovation. If not, risk strategies will be imposed by the government without your input.

The interviews are fully consented and completely confidential. No information is attributed to you, your department, or your university. Your university is aware of this study, and Lawrence Zicarese is CC'd.

I look forward to any questions you have and if you would be willing to schedule an interview.

Thank you for your consideration,

Emily

Timeline / Messages

Sep 30: Email contact from Emily Pitek:

CC'd to Lawrence Zicarese <lawrence.zicarese@stonybrook.edu>

Subject: Assistance with concerning social media requests

Hello Jan,

I am contacting you **because Stony Brook University thinks you might have observed or experienced a situation recently involving a research security risk.** Research security risks can be a situation that is questionable in nature, including activities such as theft of ideas or data, unauthorized release of prepublication research, intentional damage/destruction of research-related resources, or intentional delay of research.

We are conducting a study to learn about research security risk in academia before the government imposes risk reduction strategies without your input. The overall purpose of this study is to better understand the identification and reporting of research security risks in the academic research environment. Our research team is comprised of behavioral scientists with the MITRE Corporation, a not-for-profit organization that operates six Federally Funded Research and Development Centers (FFRDCs).

Would you be willing to participate in a 1-hour interview via Microsoft Teams or Zoom in the next week? Your insights will impact the development of research security approaches that are effective but frictionless, feasible, and support your university culture and values.

The interviews are fully consented and completely confidential. No information is attributed to you, your department, or your university. Your university is aware of this study and Lawrence Zicarese is CC'd.

I look forward to any questions you have and if you would be willing to schedule an interview.

Thank you for your consideration,

Emily Pitek

Timeline / Messages

Zoom interview Nov 9.

At the beginning of the interview, they explain the study, without explaining that the LinkedIn Emails are from them. Before I sign the consent form, I ask them why SBU might think I had such contact. They still do not disclose.

After signing, the first question is: Did you have contact in the last three weeks on LinkedIn.

At that moment, I ask them directly if they sent the message. Reluctantly, they confess. I express my displeasure, but go along with the interview. Emily promises to forward my concerns to the PI, which she does.

Timeline / Messages

After some email exchanges with the PI

Hello Dr. Bernauer,

When I am back in front of my computer, I will send you the IRB approval memo.

All of your points below were thoroughly considered by me, my research team of other experienced behavioral scientists, and an accredited IRB., as you surely do for any research that you conduct in your field. This study has previously been successfully conducted with interviews with 300 people. **Yes, the FBI is informed of and very supportive of this study.** They are extremely interested in data-driven solutions to protecting academic researchers and their valuable work. The goal is actually not more training.

I am sorry that the responses to your concerns are being perceived as dismissive. That is not the intention. I believe that is often a challenge with email so please give me a call if you wish to discuss this further.

703-983-3846

Cheers,

Deanna

Timeline / Messages

11/10, Lawrence's answer:

Good evening Jan

Thank you for meeting with the MITRE research team and sharing with me your concerns. Your time and insights into this new security risk are very much valued.

The purpose of this study is to learn from the very real experiences of faculty who receive these types of messages and identify the least burdensome way to help faculty protect their ideas and work while maintaining the open and collaborative environment needed for innovation. The three LinkedIn messages you received for this study are based on real messages being sent to the academic community as part of a new social engineering approach by bad actors. The MITRE research team does not inform the university how faculty respond or engage with the LinkedIn messages, and all information discussed in the interviews are kept anonymous and aggregated.

I am sorry you found the experience burdensome. I want to reassure that we carefully evaluated the IRB approval and MITRE is working well within the ethical human subjects federal guidelines.

I am happy to connect you with Dr. Deanna Caputo, the study PI, if you like. Please let me know at your convenience and I will connect you

Sincerely,

Larry

Thoughts

- Multiple people in P&A had these messages (Everyone who is on linkedin?)
 - While interview is (maybe) confidential, reaction can be directly observed by SBU and other parties!
 - Purpose of this study not clear. Multiple, different and illogical answers.
 - Many open questions
-
- We already have annoying fishing “test” emails. I’d rather do research than play the guinea pig.

Why is this not the same as the phishing mails?

Phishing mails are sent:

- With consent
- On university property
- Marked as phishing tests in the headers
- Most importantly: Failing is not criminal

This is not the case for the MITRE study.

Questions

1. Is the study still ongoing? Are other studies like this planned?
2. Would it be possible to get a copy of the research protocol, and the IRB review report.
3. Did MITRE contact SBU, or did SBU contact MITRE?
4. Does SBU pay for the study or is there any other monetary compensation towards MITRE?
5. What is the purpose of the study? We heard conflicting information.
6. Did SBU leadership consider asking the faculty instead? What were the reasons to not do so.
7. Who else at SBU is informed of this study? What information was shared?
8. Did SBU share a list of personnel with MITRE?
9. What information was shared with MITRE?
10. Is SBU aware who was contacted and who was not?
11. How did MITRE and SBU estimate the additional workload?
12. How did MITRE and SBU estimate the additional risk, both from a perspective of mental health and job security?
13. Does MITRE know that SBU email are not private? Was the IRB aware of this?
14. How does MITRE and SBU make sure that reactions of contacted personnel can not be inferred by SBU or other parties?
15. Is LinkedIn informed about the study?
16. What information was shared with the FBI and other federal or state agencies?
17. How many people were contacted by email with cc to Lawrence Zacarese <lawrence.zacarese@stonybrook.edu> that were not contacted over LinkedIn before?
18. Were there any steps taken to make it impossible for SBU to infer the list of contacted people and their reaction, which is directly observable by SBU.
19. Why was the deceit not revealed at the first possible opportunity, the contact email asking for an interview?
20. Why was the deceit not revealed before giving consent?
21. When would the deceit have been revealed?
22. How would people be informed of the deceit if they do not choose to take part in the interview?
23. What happens if the emails are not answered at all, i.e. might be unmonitored, and the linkedin contact is blocked? The latter might be undetectable by the sender.