The Ethical Times

Roy Koshy, Editor

Volume 27, Issue 7 — September 2025

The Problems of Others

By Alex Kipp

October is one of my favorite months in New York. Cool, crisp nights, Halloween planning, and a full four weeks to think about cybersecurity. "But wait," you might respond, "I'm pretty sure 'leaves changing colors' should be mentioned before your weird obsession with cybersecurity." And to that I say, "It's not a weird obsession. October is Cybersecurity Awareness Month, according to NYC Cyber Command." As you snap pictures of autumn leaves and fresh-picked apples and post them with heartfelt missives about life as a gossamer blip on an infinite timeline, you will no doubt be doing so with one of those phone-shaped computers we all carry around. So, it's the perfect time to tuck a thought or two about cybersecurity into our frontal lobes. We might even be able to tie those thoughts to some thoughts about ethics compliance.

We tend to think about mistakes, either in ethics or cybersecurity, as things that happen to other people, sometimes overestimating our own competency and underestimating that "other" person who made the mistake.

Of course, you are not going to respond to an email from a foreign government official who (ironically) has a pile of money he can share with you only if you send him some of yours; or reply to a misspelled text that the car you didn't know you owned has overdue tickets. If we look back nostalgically to a time ten or so years ago, these were the scams out

there. Bad actors used social engineering to take advantage of often older people with low computer literacy with refund scams like this: You get an email from Geek Squad saying you've bought a computer warranty you don't need. You call the number. They tell you they can refund the money for the warranty. All you have to do is give them remote access to your computer with AnyDesk or something similar. They ask you to access your bank accounts so they can process your refund. Then they trick you into thinking that they gave you too much back. Say $3000 instead of $300. The scammer then begs and pleads with you to return the money or he'll lose his job. It has to be done right away. But the only way to do it? Go to Target and buy him $2,700 worth of gift cards.

I, dear reader, just like you, can see the red flags a mile away. But I hope to be 75 one day. And I imagine, if I do live that long, that I will no longer be terribly computer literate. I'll definitely have some memory problems (including whether or not I bought a computer warranty). I imagine I'll constantly be on the phone for all kinds of things: Social Security (if we still have it); Medicare (if we still have it), doctor's appointments (or, maybe not, depending on Medicare); pest control; and finally getting around to cancelling my HBO MAX subscription. I imagine those customer service reps (if we still have them) will be taking me through endless, seemingly senseless steps to get a prescription filled or an appointment changed. Hmm…maybe I don't want to make it to 75? But, from this perspective, you can start to see how the Geek Squad scam is engineered to be effective with a specific kind of mark.

We see that little old lady getting duped by a caller pretending to be from Geek Squad and we think, "that will never happen to me!" But our confidence reveals a blind spot.

Because the phishing email targeted to you won't be misspelled. It won't be from Geek Squad. It's going to be socially engineered to match the shape of your job. It might contain information that seems to be of the kind that only someone who knew you could know. The email might seem to be from people you know or work with. It might mimic the kind of language you'd expect to see from a vendor or an HR Director. All of these tactics are designed to disarm you with fake cues of authenticity. And once your guard is down, it's much easier to click on the link or attachment. Scammers use increasingly sophisticated ways to create a false sense of context in order to bypass your defenses.

This notion of context reminds me of ethics violations. When I read a case of a City employee accepting an illegal gift from the member of the public, a fancy dinner perhaps, I feel very little empathy. First of all, because in my 20 years of government service, no one has ever offered to buy me dinner. But also because, in my uncharitable imagining of the way that meal went down, the mistake is glaringly obvious. In my imagining, the vendor twirls his villainous moustache as he orders another round for the table and showers the public official with hyperbolic praise as he steals the candy

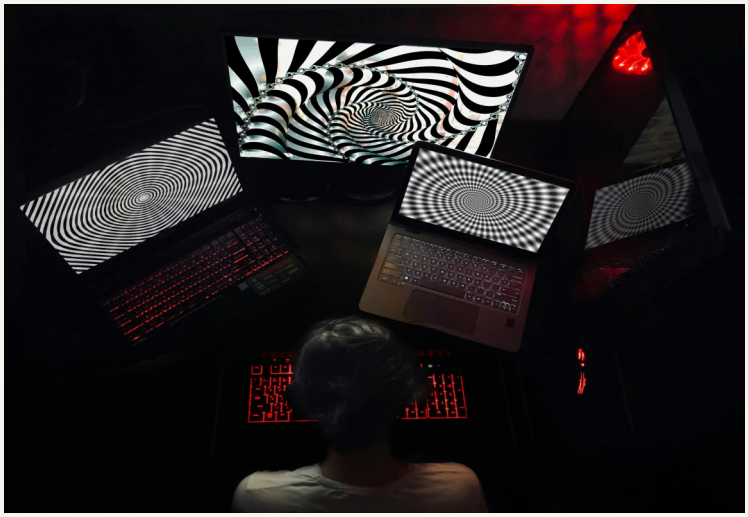
out of the mouths of small children. How could the public official not spot the attempt to influence him?? As I finish reading the case, I congratulate myself for being the kind of person who would never be so easily duped into an ethics violation.

But that's not what gift offers look like. Gifts tend to come from people you deal with. Those people might know a heck of a lot about the kind of work you do. If you work in IT, you're likely to work with tech vendors; if you're a hospital administrator, you're likely to deal with vendors who provide medical supplies and services. They'll be dressed like you. They'll speak your language. They'll smile. They'll laugh at your jokes and agree with you about how special your children are. None of this is nefarious. But it is disarming, using familiarity and friendliness to put some rose colors on something that is outright impermissible to accept.

At the end of a two-hour dinner, some nice food and fancy drinks, lots of amusing anecdotes, a little blip appears on the timeline: the bill. The vendor sweeps it up before you have time to say anything. Maybe you should keep quiet. You don't want to offend them, especially after the nice time you've shared! And besides, this little dinner is not the kind of thing that you would ever let affect your judgment. Ethics violations are things that happen to other people! My friends, in the words of the great Frank Zappa, We Are The Other People.

And like all Other People who work for City government, you may encounter a conflict of interest situation that needs confidential advice. It could be about the offer of a gift, or sitting on your co-op board, or taking a second job, starting a business, or getting involved in a political campaign. The questions can be answered by the friendly folks of the Board's Legal Advice Unit. Call 212-437-0707 and ask to speak to the Attorney of the Day (during business hours, please) or email them anytime at aod@coib.nyc.gov. And if you've got cybersecurity questions related to your City work, talk to your agency IT department or engage with the NYC Cyber Command Cybersecurity Awareness and Training (CSAT) team via their Contact form.

Alex Kipp is the Director of Education & Engagement at the New York City Conflicts of Interest Board.



NEW YORK CITY CONFLICTS OF INTEREST BOARD

nyc.gov/ethics
Phone: (212) 442-1400
Fax: (212) 437-0705

Recent Enforcement Cases

Misuse of City Time. A Custodian Engineer for the New York City Department of Education ("DOE") assigned to a school in Queens also worked as a Stationary Engineer for Kingsbrook Jewish Medical Center ("KJMC") in Brooklyn. During the more than three years he was employed by KJMC, the Custodian Engineer would leave his DOE school before the end of his DOE workday to commute to and perform work for KJMC. To resolve disciplinary charges brought by DOE for this conduct, the Custodian Engineer agreed to resign and forfeit more than $30,000 of accrued annual leave. In a subsequent and separate settlement with the Board that took into account the penalties the Custodian Engineer had already incurred, the now-former Custodian Engineer agreed to pay a $3,000 fine.

Misuse of City Time. A DOE Social Worker had a second job with online therapy provider Talkspace. At times when she was required to be performing work for DOE, she conducted a therapy session for Talkspace and used a Talkspace application to make changes to five other scheduled appointments. The now-former Social Worker agreed to pay a $1,500 fine.

Misuse of City Time & City Resources; Prohibited Appearances; Misuse of City Position. A Pupil Accounting Secretary at a DOE school in Brooklyn had a second job at TEiAM, a not-for-profit organization that provides afterschool programming at DOE schools. The Secretary used City resources—her DOE email account on 20 occasions and a DOE scanner on six occasions—to perform work for TEiAM, and she sent 10 of those emails at times when she was required to be performing work for DOE. She also communicated with DOE employees on behalf of TEiAM on 12 occasions and initiated a $20,000 purchase order for TEiAM services at her own school. The Secretary agreed to pay a $4,500 fine.

Misuse of City Resources. An Assistant Deputy Warden for the New York City Department of Correction ("DOC") went to Rikers Island in the middle of the night to use a DOC color copier to print copies of a pamphlet/itinerary for her wedding. The Assistant Deputy Warden agreed to pay a $1,000 fine.

Prohibited Political Activities. The Chief of Staff to a City Council Member sent a text message to seven of his subordinates asking them to donate to the Council Member's reelection campaign. After receiving the text message, four of the seven subordinates made donations totaling $200. The Chief of Staff agreed to pay a $2,250 fine.

Visit our **search engine** for all COIB Enforcement Dispositions.