Common Email Scams

Common Email Scams

Sometimes phishing emails can be hard to spot because they aren't asking you to click a link or download an attachment. This article discusses some common email scams that try what's often called "social engineering" - they pretend to be someone or know something in order to manipulate you. Often these scams are financial in nature. The FBI has more information on commonly seen scams available on their website.

> You can help us protect others at the Institute: If you receive a phishing email please report it (using the Phish Alert Button or forward it as an attachment to phishing@mit.edu). If you receive an email you aren't sure about, please don't hesitate to ask. If you report using the Phish Alert Button, please leave a comment with your question. If not, please forward the email as an attachment to security@mit.edu and include your question.

TOAD - Telephone-Oriented Attack Delivery

You get an email receipt for something you didn't purchase, and all the links don't work, but there is a phone number that they want you to call.

These scams often impersonate companies like Norton, Geek Squad, PayPal, or McAfee and the fake call centers can be very convincing. If you call the number, they will want to verify financial details, and sometimes will ask you to install software to allow them to remotely access your computer to "fix" a problem. This instead is a way for them to install malware and steal data. If you are unsure that the receipt or invoice is fake, you can always report it to phishing@mit.edu and/or contact the given company directly via the customer service number on the company's website.

Are you free at the moment? Let me know ASAP.

You get a short email from someone in your organization, usually a higher-up, saying that they need you to respond ASAP. If you respond, usually they ask you to purchase gift cards or wire money somewhere.

The scammer has just spoofed the email address that it appears to be coming from (often just changing the display name), not compromised any account. Often scammers will target an entire lab, one person's direct reports, etc. The MIT organization structure is openly available on our websites which makes it easy for scammers to get contacts. Variants of this scam have hit many universities.

The conversation goes something like this:

> *From: Tim Beaver <tbeaver.mit.edu@domain.com>*
>
> *Hello,*
> *I would like to know if you are free at the moment? Let me know ASAP.*
> *Regards*

If you reply, you might receive something like:

> *I'm currently in a Conference meeting right now but there something i must handle and its very important, that's why I'm contacting you through here. I should have called you but phone is not allowed to be used during the meeting. I don't know when we are going to be through from this meeting and I want you to help me out on something very important right away*

And then...

> *Great, thanks!*
> *i need you to help me get an iTunes gifts card from the store,i will reimburse you back when i get to the office.*
> *I need to send it to someone and it is very important cause i'm still in a meeting and i need to get it sent Asap.*

> *Ok. The amount I want is $100 cards by 5 pieces or $50 cards by 10 pieces, So that will make it a total of $500, I'll be reimbursing back to you. I need physical cards which you are going to get from the store. When you get them, just scratch each card at the back and take a picture of them and attach it to the email then send it to me here. Just hold on to the cards. I'll get them from you later.*

I know your password is <someoldpassword>

This is what's considered a "sextortion" scam. In this version, the scammers use old compromised passwords to make the scam more credible. They claim to have installed malware on your computer and to have captured a video while you were visiting adult sites

If you receive one of these emails, you may recognize the password as one you have used in the past. The passwords are from old data breaches and are compiled into combo lists like the Anti-Public list . There is no such malware on your computer and no video exists.

> If you are still using this password anywhere, you should change it immediately! Consider using a password manager like LastPass to help you generate and store unique passwords for all your accounts

While this scam email is a hoax, the FBI recommends the following steps to avoid becoming a victim of sextortion:
• Never send compromising images of yourself to anyone, no matter who they are — or who they say they are.
• Don't open attachments from people you don't know, and in general be wary of opening attachments even from those you do know.
• Turn off (and/or cover) any web cameras when you are not using them.

> *I will cut to the chase. I do know someoldpassword is your password. More to the point, I know about your secret and I've evidence of it. You do not know me and nobody hired me to investigate you.*
>
> *It's just your bad luck that I stumbled across your blunder. Let me tell you, I actually installed a malware on the adult vids (sex sites) and you visited this web site to experience fun (you know what I mean). When you were busy watching video clips, your browser started out operating as a Rdp (Remote control desktop) with a key logger which gave me access to your display screen and also webcam. Right after that, my software program obtained all your contacts from your messenger, facebook, as well as e-mail.*
>
> *After that I put in more time than I probably should have investigating into your life and generated a two screen video. First part displays the recording you had been viewing and 2nd part shows the recording of your web cam (its you doing dirty things).*
>
> *Frankly, I want to forget details about you and let you move on with your daily life. And I will offer you two options that can accomplish that. These two choices either to ignore this letter, or just pay me $2900. Let's understand these two options in more details.*
>
> *Option One is to ignore this email message. Let's see what will happen if you pick this option. I will definitely send out your video to all your contacts including relatives, coworkers, and many others. It will not shield you from the humiliation your family will feel when relatives and buddies find out your unpleasant details from me.*
>
> *Other Option is to send me $2900. We will call it my "privacy charges". Now let me tell you what happens if you choose this path. Your secret remains your secret. I will delete the recording immediately. You continue on with your daily life like nothing ever happened.*
>
> *At this point you may be thinking, "I will complain to the police". Without a doubt, I have taken steps to ensure that this e-mail can't be traced returning to me and it won't prevent the evidence from destroying your daily life. I am not trying to steal all your savings. I just want to be paid for my efforts I placed into investigating you. Let's hope you decide to make pretty much everything disappear completely and pay me my confidentiality fee. You'll make the payment via Bitcoins (if you don't know this, search "how to buy bitcoins" in google)*
>
> *Required Amount: $2900*
> *Bitcoin Address to Send to: <bitcoin address>*
> *(It is case sensitive, so copy and paste it)*
>
> *Tell nobody what you would use the bitcoin for or they possibly will not give it to you. The procedure to have bitcoins will take a day or two so do not delay.*
> *I've a special pixel within this email, and now I know that you've read this message. You now have 24 hours in order to make the payment. If I don't receive the BitCoins, I will definately send out your video to your entire contacts including relatives, colleagues, and many others. You better come up with an excuse for friends and family before they find out. Nonetheless, if I receive the payment, I will erase the video immediately. It's a non negotiable one time offer, so please don't ruin my personal time & yours. The clock is ticking.*

Your account is hacked!

This is a variation on the sextortion scam. In this one, they've spoofed your email address to make it look like it is coming from your account. They claim that they have hacked your account, installed malware, and captured sensitive information that they will make public unless you pay a bitcoin ransom.

> *From: <target_user@mit.edu>*
> *Subject: target_user@mit.edu was hacked*
> *Date: October 14, 2018 at 6:48:09 AM EDT*
> *To: <target_user@mit.edu>*
>
> *Hello <target user>*
>
> *My nickname in darknet is <some random thing>.*
> *I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.*

> *Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.*
>
> *I have access to all your accounts, social networks, email, browsing history.*
> *Accordingly, I have the data of all your contacts, files from your computer, photos and videos.*
>
> *I was most struck by the intimate content sites that you occasionally visit.*
> *You have a very wild imagination, I tell you!*
>
> *During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.*
> *Oh my god! You are so funny and excited!*
>
> *I think that you do not want all your contacts to get these files, right?*
> *If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created.*
>
> *Send the above amount on my bitcoin wallet: 1MN7A7QqQaAVoxV4zdjdrnEHXmjhzcQ4Bq*
> *As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.*
>
> *Otherwise, these files and history of visiting sites will get all your contacts from your device.*
> *Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!*
>
> *Since reading this letter you have 48 hours!*
> *After your reading this message, I'll receive an automatic notification that you have seen the letter.*
>
> *I hope I taught you a good lesson.*
> *Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!*
> *Good luck!*

Looking for a tutor at "your location"

This scam usually targets students, but sometimes faculty as well. You receive an email from someone who does not live locally but is looking for someone to tutor their child while they travel to "your location." Once they hire you, they will send you a check for more than the agreed upon rate for the lessons and ask you to send the excess somewhere else, usually to help pay for the child's travel costs. They hope that you will send the real money on before their original check has a chance to bounce.

> *Hello,*
>
> *During my search for a lesson teacher that would help in taking son (Kenneth) During is stay in your location. I found your advert and it is very okay to me since you specialize in the area I'm seeking for him, My son would be coming to your city before the end of this month for a period of time with his friend, I'll like to know if you can help in taking him for the lesson? just to keep him busy and refresh. Kenneth is 11 years old, So kindly let me know your charges per hour/lesson in order for me to arrange for his payment before he travels down to for the lessons to commence.*
> *He will be staying there for 2 weeks and Please Reply back on:*
>
> *(1). Your charges per 2 hours (3 times a week for 2 Weeks):starting from 7th September until 20th September 2018*
>
> *(2) Total Cost For 6 class/12 hours lessons in 2 Weeks*
>
> *(3). The Day you will be available to teach him During the week:*
>
> *Well am very happy that i see you as my son tutor and about your years of Experience there is no problem about the lessons, My son will be coming with his caregiver. So there is no problem for the lesson to commence by next week, my son caregiver will be bringing him to your location for the lessons and you can teach him anywhere around you including the Library or your home if that is okay by you so i will like you to teach my son the best of you when he get to the city for the lessons. I will like you to email me with your schedule for the lessons, I will like you to email me with the name on the check and Full mailing address where the check will be mailed to and including your Home and Cell phone number for my attorney to issue out a check to your before leaving the the state, by this week, I will be awaiting to read from you soon with your name and address.*

Pet sitting

This is similar to the tutor scam. In this case the job is pet sitting, and they may even use a compromised account or pretend to be a fellow student. For example "My uncle is looking for a dog sitter, please email him at ...." The scam is similar in that they will try to send you a check for more than the agreed upon rate for the pet sitting and ask you to send the excess somewhere else. They hope that you will send the real money on before their original check has a chance to bounce. In this example, they are also asking you to send them a copy of your ID.

> Do not send a photo of your MIT ID card, Driver's License, or Passport to anyone via email for a job application. If you find you have fallen for this scam, please contact the IS&T Security team at security@mit.edu. If you sent your Driver's License or Passport you should consider a freeze of your credit.

> *Subject: PET-SITTER NEEDED.*
>
> *Hello,*
>
> *I am putting out this Ads for my uncle..he just got transferred here and needs someone (STAFF/STUDENT) to pet-sit his 4months old puppies twice a week. The pay is $300/weekly. Contact him on (l.pcanepa19558@gmail.com< l.pcanepa19558@gmail.com>) with your Names and Phone number for easy communication. If you are not interested, kindly refer someone who you think would be interested.. your referral would be appreciated, Thanks.*

If you email the "uncle" about the job, you would receive a reply like this:

> *Hello <target email>,*
>
> *I am in receipt of your mail along with information's provided as requested in my previous mail, its my pleasure to work with you as you take-on responsibility of taking care of my puppies.*
>
> *After a thorough review of your application, I have selected you for the service of taking care of the dogs at the agreed time.. I want to make sure you have everything you need to do your job and for this reason, I am putting in some measures to this effect.*
>
> *My wife have made proper arrangement for items and food and furniture's for the puppies to enable you do your job easily.*
>
> *She has ordered the below items so as to make your job easy,*
>
> - *Food (dry food, wet food and treats) and bowls.*
> - *Medications, including when and how much to give.*
> - *Toys.*
> - *Harnesses and leashes.*
> - *Grooming supplies, such as shampoo, brushes, toothbrushes and toothpaste.*
> - *Cleaning supplies, such as paper towels and an enzymatic cleanser.*
> - *Furniture.*
>
> *My plan is to have someone available to do this pet-sitting job before my arrival, so I can easily settle down with my job,this is why I am making sure all is done to secure your services before my arrival.*
>
> *To secure your services before my arrival my employee will be sending you a check in the amount of $3,380, this is to cover your first week pay of $300 and the balance funds should be sent to the clerk who will purchase the items and have them in place to help us settle in quickly when we arrive.*
>
> *Upon your receipt of the check,I will let you know how to go about the balance for the above listed items my wife has ordered.I will count on you and your words as I hope we will have a nice time working together.*
>
> ***NOTE:** I will dropping off my puppies in your apartment on the days you are to watch after them.....if this is not fine with you I can let you stay with them at my apartment.Let me know which best suits you.*
>
> *I will let you have my home address as soon as I arrive.I would also appreciate any form of identification via email attachment in your next mail.*
>
> *Find attached to this mail a copy of my International Passport.*
>
> *I will need you to confirm your below details to me in your next mail,*
>
> **NAME ON CHECK - **
>
> **MAILING ADDRESS - **
>
> ***City -State -Zip code -***
>
> ***PHONE NUMBER -***
>
> *I need you to validate your above details to enable my employee write you a check.*
>
> *I await your response to this mail so I can forward your details to my employees for payment to be mailed to you next week.*
>
> **Lastly provide me any form of Identification Drivers License or any form of identification in your next mail.**

Thanks,
Larry P.