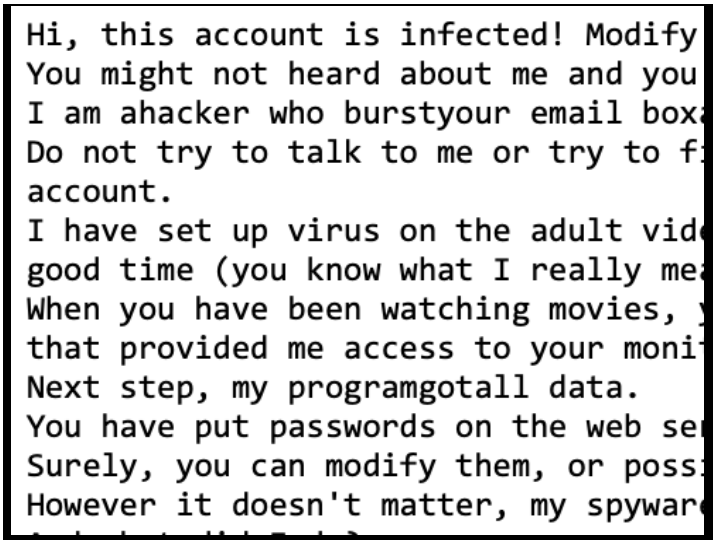
Email Safety

Several popular email scams and threats are cycling through inboxes; this is a great time to review email security tips.

The first email we reference is the "sextortion email scam." This email alerts you that your password has been stolen and that the attacker has gained access to your computer. The attacker also enters into a blackmail scheme and requests Bitcoin, claiming that he/she has evidence of pornography on your computer.

Has your password really been hacked? **Yes.**
Your password was likely compromised in a recent breach (MyFitnessPal, Experian, DropBox, etc.) and posted online. If the sextortion email mentions a specific password, and it was a password that you used, you should stop using that password on ***all*** websites.

Sextortion Email Scam


Hi, this account is infected! Modify
You might not heard about me and you
I am ahacker who burstyour email box
Do not try to talk to me or try to f
account.
I have set up virus on the adult vid
good time (you know what I really me
When you have been watching movies,
that provided me access to your moni
Next step, my programgotall data.
You have put passwords on the web se
Surely, you can modify them, or poss
However it doesn't matter, my spywar

Does the attacker have access to my computer? **No.**
How should I proceed? Delete the email. If a specific password was mentioned, stop using it immediately and never use it again. Visit: **https://haveibeenpwned.com/** to check a registry of email addresses and passwords that have been hacked and posted online.

The second email is one we call "Fake Boss Requests." In these emails, company executives appear to ask for assistance with bank transfers or purchasing gift cards.
When these emails hit your inbox, they really do look like they are from within the company at first glance. In most cases, another look at the email address/sender information reveals a mismatch, or the grammar/spelling within the email message may seem off.

Recently these requests have become more sophisticated, warning the employee to not call the boss to check-in, as the boss is too busy and needs the transaction completed quickly.

Fake Boss Request Scam

-----Original Message-----
From: [redacted] <private66@stny.rr.com> Employer Email from fake address
Sent: Friday, March 8, 2019 10:16 AM
To: [redacted] Employee Email
Subject: Re: RE: RE: Icards..

Ok. I'll need 8 pieces of $200 face value/each =$1600 eBay Gift Cards, scratch-off silver lining at the back of the card to reveal the codes.Send a clear picture of the pin codes on all cards to 573-246-0714.. His name is Jason.
---- [redacted] Employee Email wrote:

I'll let Allison know and I can run right now, how much are you looking to get?

-----Original Message-----

From: [redacted] Employer Email

Sent: Friday, March 8, 2019 10:11 AM

To: [redacted] Employee Email .com>

Subject: Re: RE: Icards..

I'm in the middle of a conference call and I need you to run an errand for me at any Target, Walmart or CVS around you. I need some eBay gift cards to send out to a client today. I'll reimburse you later today and Let me know how soon you can get them.

How Should I Proceed?
If an email request seems odd or out-of-character, personally contact the sender via phone or face-to-face to ask about the requested transaction. Replying via email is not always a safe choice, as you may be replying to the scammer's email address and not the address of your coworker.