How to detect possible eMail scams

I've written about internet scams that pop-up in your browser through adware that's been injected into websites but wanted to talk now about scams that can show up in your eMail inbox and how you might be able to sleuth them so you don't get taken in.

These eMails may have the "appearance" of legitimacy and authority. They are often written in such a way as to imply that immediate action needs to be taken in order to avoid, for example, unauthorized access to some eMail, iTunes or iCloud account, payment or charge.

I'm going to show a few examples and offer some suggestions and tips on how you can recognize these kinds of messages and what you should do about them when you suspect you may have received one.

My first tip is just this: Slow down, don't panic.

The sender of the eMail is hoping that this is exactly what you will do…respond quickly before you've taken a moment to think about what is being asked and to do something before your skeptical guard goes up. They are hoping you panic. Don't give them the satisfaction.

Never click on a link embedded in a suspicious looking email!

In fact, best practice is ALWAYS to manually type in the URL (website address) in the address bar of the browser you use (Safari, Firefox, Chrome, Explorer) if you think the eMail "might" be legitimate and want to check it out.

It's a pretty trivial thing to mask a link and have it redirect to a completely different site. Without your knowledge you've been directed to a place that has the appearance of legitimacy and are now being asked to enter your personal information like eMail, passwords, social security number, etc.

Here's an example I created in just 10 minutes. Click the link to see how easy it is to spoof a site and make the page you're linking to look legitimate.

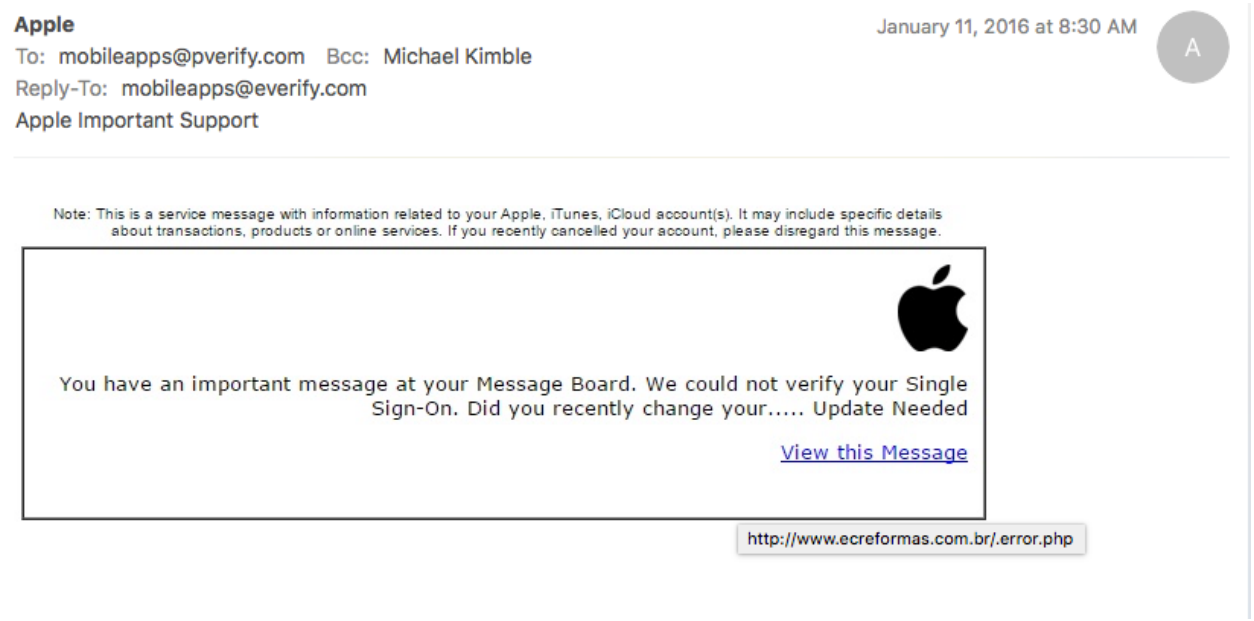
Click here to update your account information: www.appleaccountinfo.com

I did a quick clip from Apples website to create this page. I could have spent more time adding the appropriate links to Apples official pages across the menu bar and in the footer to be even more convincing.

Just to reiterate.

Unless you know and trust the sender, don't click on an embedded link in an email and then use that page to submit personal, account and passwords, and financial information.

Let's take a look at a couple of scam eMails I've received:



There are a lot of red flags with this message.

1) I've never heard of having "an important message at my Message Board" from Apple, I don't know what the "Message Board" they might be referring to could be.

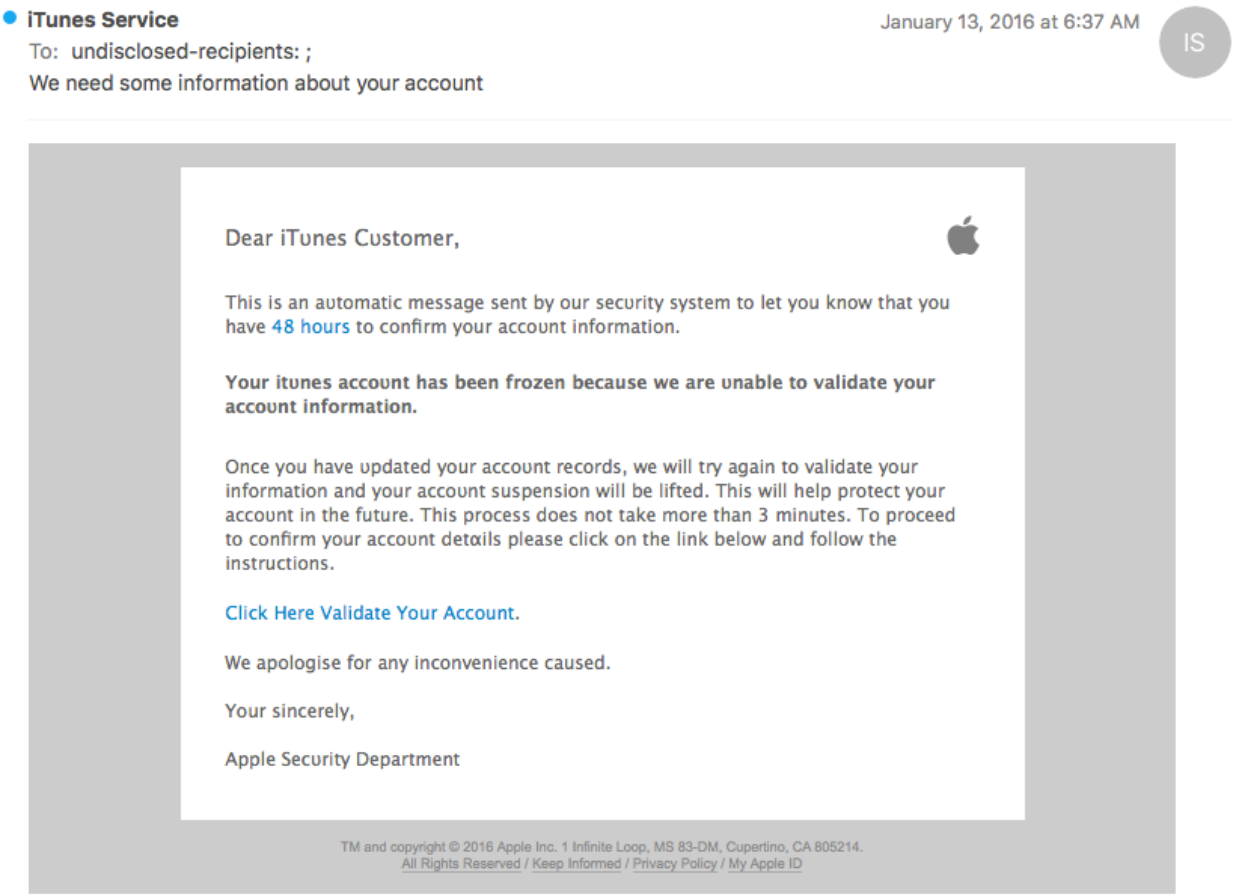
Do not click on "View this Message"

2) The email is addressed to "mobilesap @verify.com" and not to me directly. I'm listed as Bcc. That's a big Red Flag.

3) The subject line makes no sense and conveys no real information. It's not a properly formed sentence.

The small print and Apple logo are just cut and paste to add the look of legitimacy.

This next eMail looks even more impressive…



1) One of the biggest red flags is when an eMail is addressed to “undisclosed-recipients.” That should be all you need to know that this is part of a bulk email meant to cast a wide net. Apple knows who you are. So does Google, your bank or any company you do business with.

2) The email implies you have just 48 hours to confirm account information. This is designed to panic you into responding right away. The assumption is that because you might not check your emails right away you actually have less than that time to respond. Better do it now!

They then inform you that your account has been frozen. So I guess you don’t have 48 hours to confirm your account information after all.

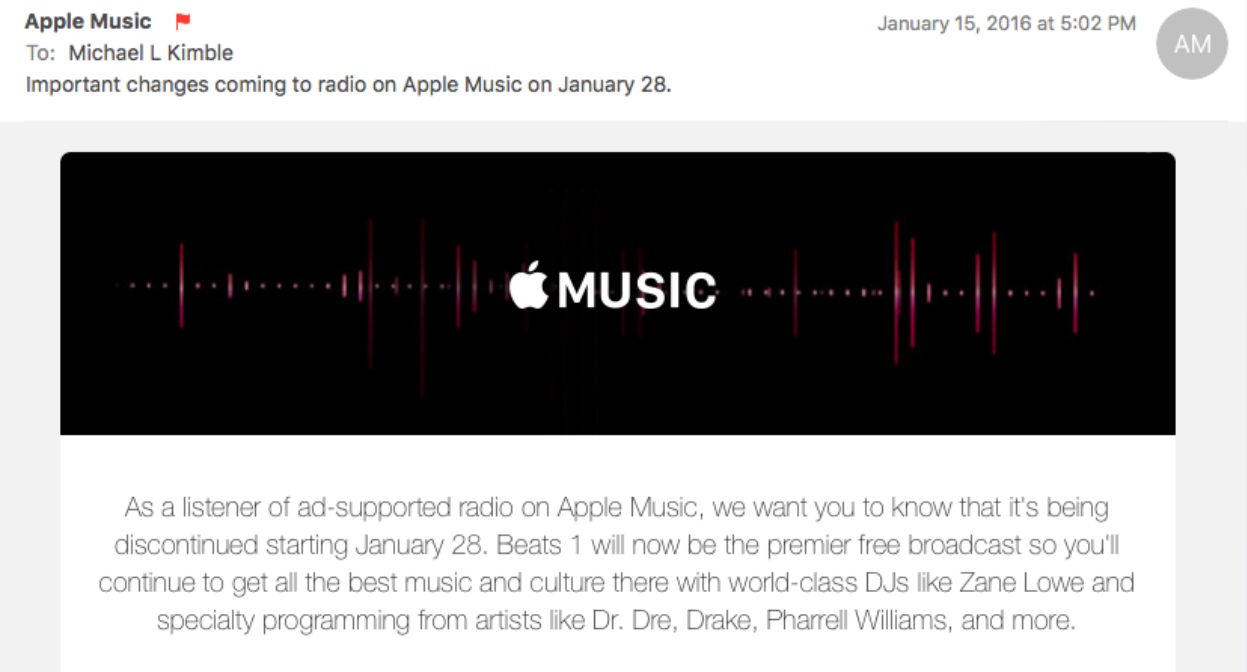
The letter doesn’t tell you what will happen if you don’t respond. A legitimate email wouldn’t threaten you in this way.

3) I’m going to say it again: Please do not click on “Click Here Validate Your Account.” Did you notice that sentence wasn’t written properly?

4) “Your sincerely,”? I probably would have written “Sincerely yours,”

Errors in grammar and spelling coming from a company as big as Apple would be another big red flag.

Let's take a look a legitimate eMail from Apple now.



1) Apple knows who I am. In fact, if I click on this email it is addressed to the one eMail account that Apple will always communicate with me on. My iCloud account. It is mkimble1@mac.com.

That's another way to check the legitimacy of an email addressed to you. If the above email were sent to one of my other email addresses I would be very suspicious.

2) The subject line contains a good summary of what the contents of the message will be. It is enough information to allow me to decide whether or not I even need to read the message.

That is something all of us need to remember whenever we send emails. Your subject line should be a short summary of the contents of the email you are sending.

3) The body of the message is clearly written. It makes no demands. Implies no threats.

Finally, here's a good one…

Yep, this is legit! Gonna claim my donation right now! I just need to give them my social security number and bank account id.

Yusun Hu
To: Undisclosed recipients: ;
Hello

You have a donation from a mega million winner, for more information kindly reply immediately.

Thank you,
Your sincerely,
Evelyn Ira Curry.

Hey, it's our friend "Your sincerely" again! And Undisclosed recipients! And our buddy from China, Yusun Hu! And run on sentences!

Things you can do when you just aren't sure:

1) Google it. See if there is information about the email you received on the internet. Some internet scams can be researched at snopes.com.

2) If you still aren't sure, visit the companies website and look for a customer service number you can call. If it's your bank or credit card company, call the number on your statement and talk to a customer service rep. If it appears to be from Apple call Apple customer service or go to the Apple Store.

3) If anyone asks for your password, don't give that up. Most companies have the ability to reset your password and can issue a temporary password. That would allow you to get into your account and settings page and make whatever changes you need to make manually.

4) Have them mail any information to you to the address on file. If they don't know that, ask them what address they do have on file. That will serve as a check to how up-to-date their data is or if they are fishing for information from you. Do not voluntarily give them any of your personal information.

I never give out my social security number or bank account information to anyone over the phone unless I am certain of the people that I am calling and talking to.

5) eMail me with an example and I can do the research for you. I'll do my best to find out what I can for you.

I hope this has been somewhat helpful to you. If you have any questions, please let me know.

Yours,

Michael Kimble

MacHelp4Me

PS - I recently received an email wanting to confirm my iPhone FCC ID number with an embedded link to “Confirm Here.” This is also not a legit eMail.