NATIONAL CYBERSECURITY ALLIANCE

IMAGETEC

TO CLICK OR NOT TO CLICK: THAT IS THE QUESTION

One thing is certain when it comes to cyber crime, email is the most effective way for criminals to deliver malware to an unsuspecting victim. Increasingly, text-based threats are rising as more people do more on mobile devices. If you are even a little bit suspicious of a text message or email--do not click. Immediately delete.

TAKE-ACTION TIPS

VERIFY TO CLARIFY

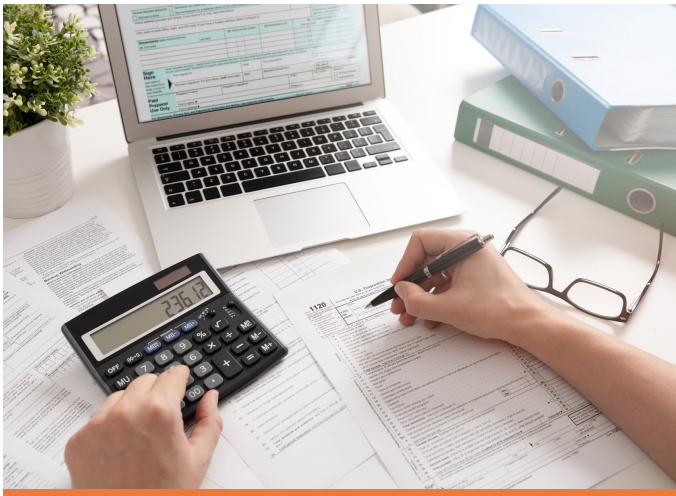
If you receive an email or text message requesting you to confirm or submit financial information, your login information, or any other sensitive personal information by clicking a link, don't. Immediately contact the organization (not via the contact information contained in the email) to verify the request. You can also visit the company's legitimate website and log into your account to see if you have any messages or action items.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, texts, posts, social media messages and online advertising are an easy way for cyber criminals to get to you. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Essentially, don't trust links.

STRANGER DANGER

Remember what you learned about not accepting candy from strangers? Apply that to the online world as well. Do not click links in emails, text messages, chat boxes, etc. from people you do not know--and be suspicious of links sent from those you know as well.



WHAT IS MALWARE?

Malware, or "malicious software," is designed to damage and destroy computers and their systems. Examples of common malware you may have heard of include: viruses, worms, Trojan viruses, spyware, adware, and ransomware.

NATIONAL CYBERSECURITY ALLIANCE

IMAGETEC

TO CLICK OR NOT TO CLICK: THAT IS THE QUESTION

TAKE-ACTION TIPS

READ THE EMAIL OR TEXT CRITICALLY

Is the sender asking you to do something they wouldn't normally ask you to do, such as bypass your company policy? Does it seem weird the credit card company is asking you to verify your credit card number or SSN? (yes--they have that information already). Are there misspelled words or unusual phrases? Is there a sense of urgency--requesting you click now or act immediately? These are often context clues in the body of the email or text hinting that something is not right.

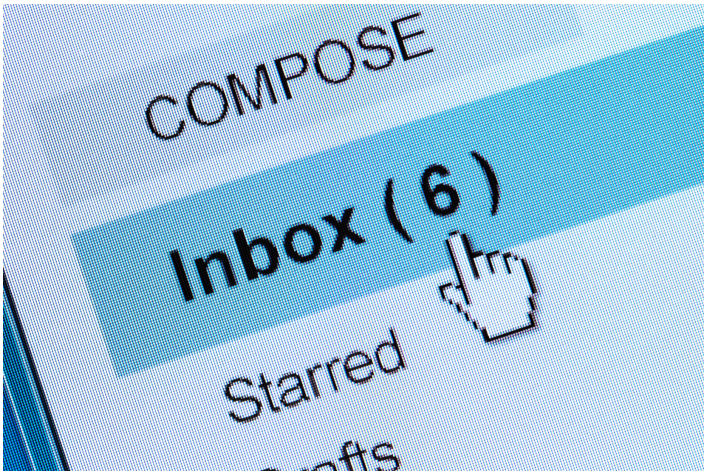
UNSUBSCRIBE MIGHT SUBSCRIBE YOU TO A HACK

Sometimes the call to action in an email can trick you--such as "unsubscribe" or "reply to stop receiving these messages." It is better to just delete the email or mark it as spam if it is spam.

A FEW TRICKS

IN YOUR EMAIL ACCOUNT, CONFIGURE THE SETTINGS SO THEY DISPLAY THE SENDER'S EMAIL ADDRESS AND NOT JUST THEIR DISPLAY NAME

This will help you verify the sender's email address is legitimate (for instance info@staysafeonline.org (correct) vs. info@staysafe0nline.org (incorrect)--notice the one simple change from an o to a 0.



PLUG-IN ASSISTANCE

There are some plug-ins you can use in your internet browser that will display a URL's true path. You might consider enabling that security feature in your internet browser's security settings.

NATIONAL CYBERSECURITY ALLIANCE

IMAGETEC

TO CLICK OR NOT TO CLICK: THAT IS THE QUESTION

A FEW TRICKS

HOVER TO DISCOVER
You can put your cursor on top of the link (be careful not to click!). When you do that, the true path will appear. Does the destination of the link align with what you would think? If it doesn't look legitimate, do not click. Immediately delete the email.

WHAT ARE YOU HIDING?
Often, hackers will use shortened URLS to make a malicious link appear safe to click. If you receive a short URL, there are free online tools where you can copy and paste the short URL into the tool and it'll expose the true path. Be careful with this, though. You don't want to accidentally click the URL. If you are afraid of copying and pasting, just delete the email or text message with the shortened URL and go to the company's main site itself to access whatever deal or event you're trying to access.

HAVE ANTI-MALWARE AND ANTIVIRUS INSTALLED ON ALL OF YOUR DEVICES
You can even install it on your phone. This will add an extra layer of protection, though it won't replace you needing to be cautious and vigilant.

ADDITIONAL RESOURCES

- **Google**: Free Phishing Quiz
  https://phishingquiz.withgoogle.com/
- **CISA:** Avoid Phishing & Social Engineering Attacks
  https://www.us-cert.gov/ncas/tips/ST04-014
- **NCSA & Adobe**: Phishing & Ransomware Video
  https://staysafeonline.org/blog/security-awareness-episode-4-phishing-and-ransomware/