How to Test a Suspicious Link Without Clicking It

Does that link look fishy? Here's how to tell if it's dangerous

What to Know

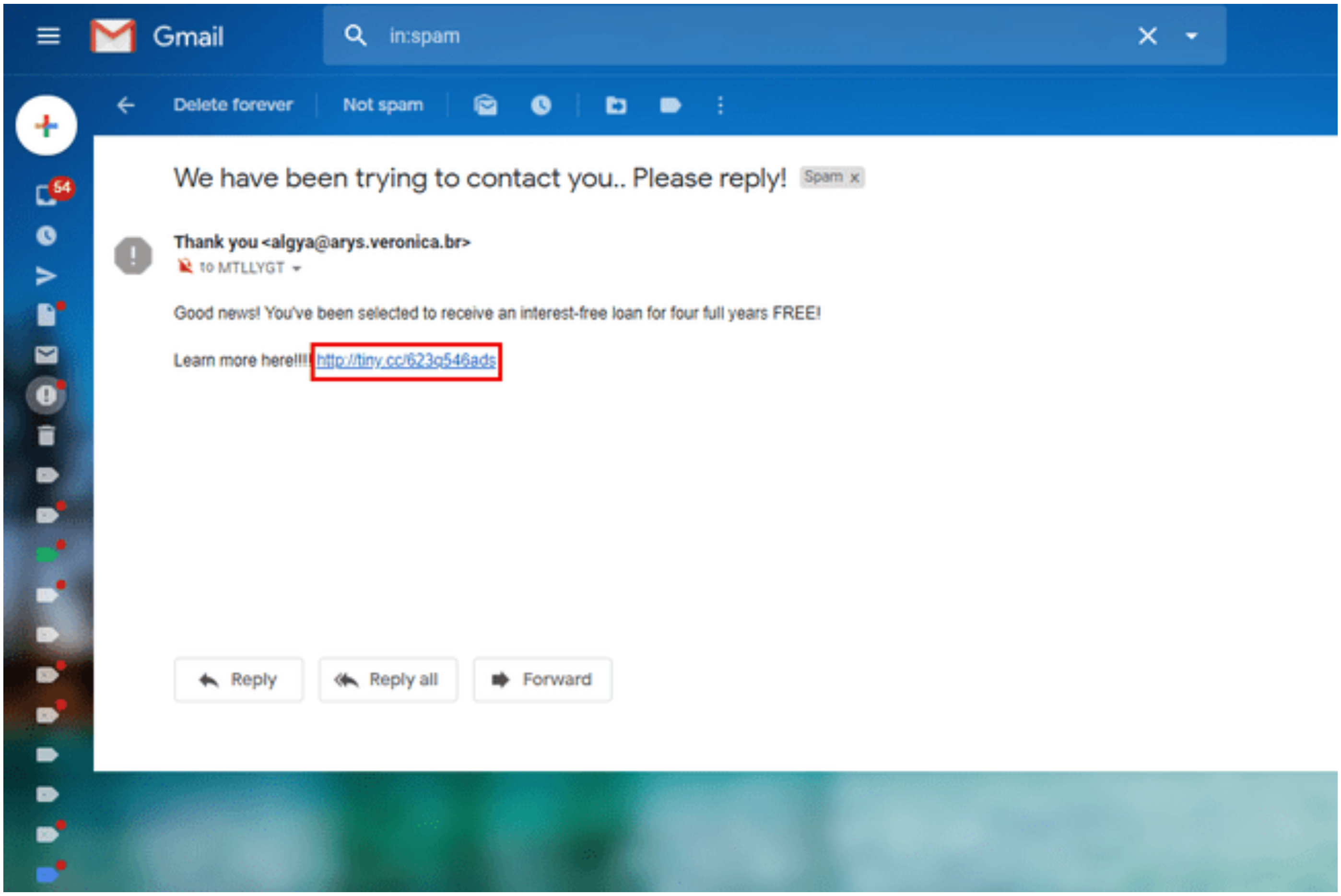
Inspect short links using a link-expansion service, such as ChecShortURL, or a browser plug-in to show the link's destination.
Verify solicited emails from your bank or other financial institution by contacting them directly. Don't click any links in the email.
Decode links with strange character strings with a URL decoding tool, such as URL Decoder, to see the real destination.

This article explains how to test a suspicious link without clicking it. It focuses on expanding short links, verifying unsolicited emails, and decoding links with strange character strings. It includes information on general safety tips for avoiding suspicious links using link scanners and anti-malware or antivirus software.

Inspect Short Links

One clue that your link may be dangerous is that the URL seems too short. While link-shortening services such as Bitly are popular and common tools for creating shorter links, malware distributors and phishers use link shortening to conceal their links' true destinations.

You can't tell if a short link is dangerous just by looking at it. Use a link-expansion service such as ChecShortURL to reveal a short link's true intended destination. (Visit the ChecShortURL website for more information.) Some link-expander sites even tell you if the link is on a list of known "bad sites." Another option is to load a browser plug-in that will show you a short link's destination if you right-click on the short link.



We have been trying to contact you.. Please reply!

Thank you <algya@arys.veronica.br>
to MTLLYGT

Good news! You've been selected to receive an interest-free loan for four full years FREE!

Learn more here!!! http://tiny.cc/623q546ads

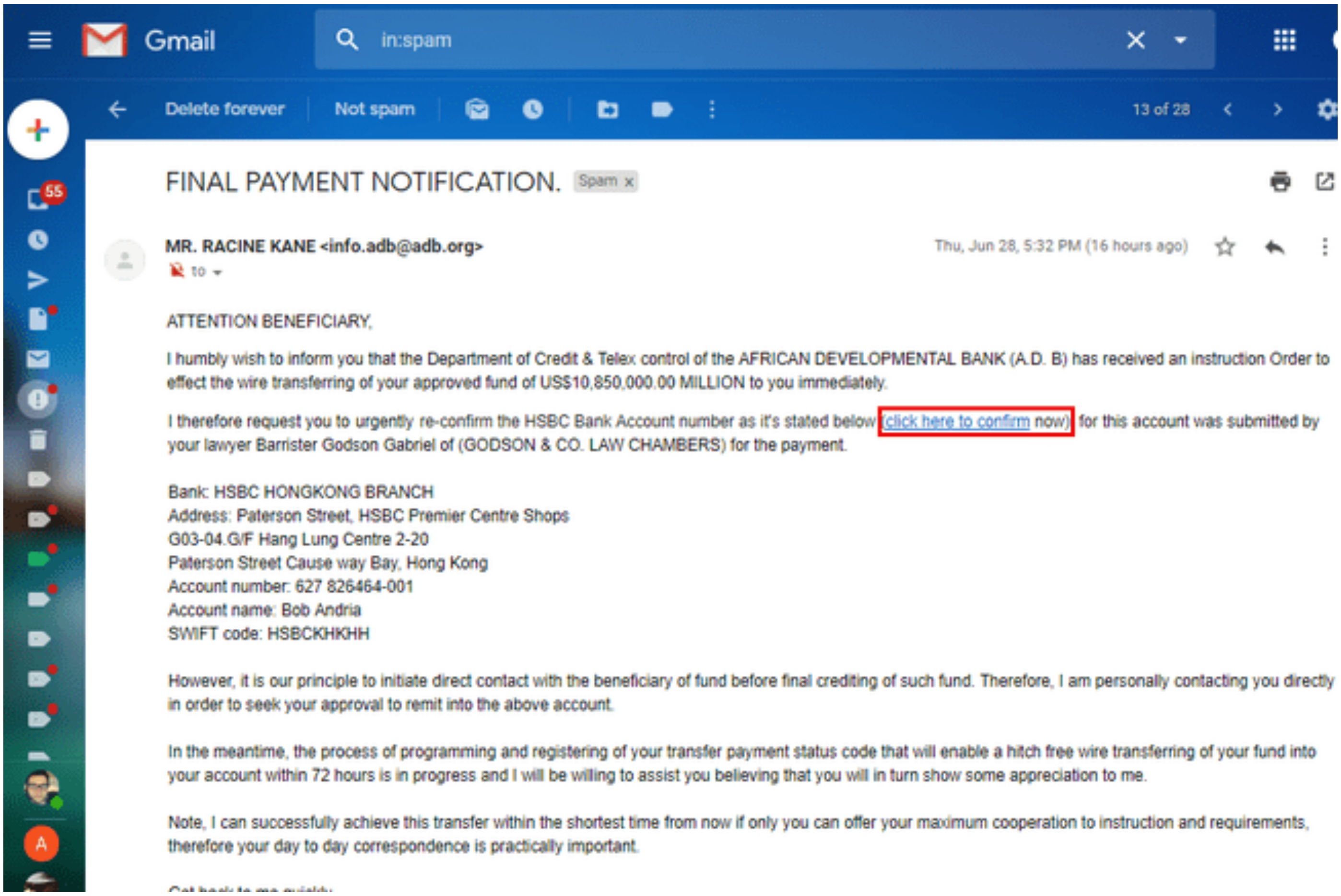
If you're dealing with an embedded link, you can't see the URL automatically. Hover your cursor over the link to reveal the URL without clicking on it and accessing its destination site.

Verify Links in Unsolicited Emails

A common phishing ploy is to send an email that seems as if it comes from your bank. These emails usually instruct victims to "verify your information" by clicking a link, ostensibly to go to the bank's website.

If you received an unsolicited email that is supposedly from your bank asking you to click a link, then you are likely the target of a phishing attack.

Even if the link to your bank looks legitimate, don't click it. Visit your bank's website through your web browser, either by entering its address or accessing a bookmark. This advice holds true for unsolicited texts from your "bank," as well.



FINAL PAYMENT NOTIFICATION.

MR. RACINE KANE <info.adb@adb.org>
to

Thu, Jun 28, 5:32 PM (16 hours ago)

ATTENTION BENEFICIARY,

I humbly wish to inform you that the Department of Credit & Telex control of the AFRICAN DEVELOPMENTAL BANK (A.D. B) has received an instruction Order to effect the wire transferring of your approved fund of US$10,850,000.00 MILLION to you immediately.

I therefore request you to urgently re-confirm the HSBC Bank Account number as it's stated below (click here to confirm now) for this account was submitted by your lawyer Barrister Godson Gabriel of (GODSON & CO. LAW CHAMBERS) for the payment.

Bank: HSBC HONGKONG BRANCH
Address: Paterson Street, HSBC Premier Centre Shops
G03-04.G/F Hang Lung Centre 2-20
Paterson Street Cause way Bay, Hong Kong
Account number: 627 826464-001
Account name: Bob Andria
SWIFT code: HSBCKHKHH

However, it is our principle to initiate direct contact with the beneficiary of fund before final crediting of such fund. Therefore, I am personally contacting you directly in order to seek your approval to remit into the above account.

In the meantime, the process of programming and registering of your transfer payment status code that will enable a hitch free wire transferring of your fund into your account within 72 hours is in progress and I will be willing to assist you believing that you will in turn show some appreciation to me.

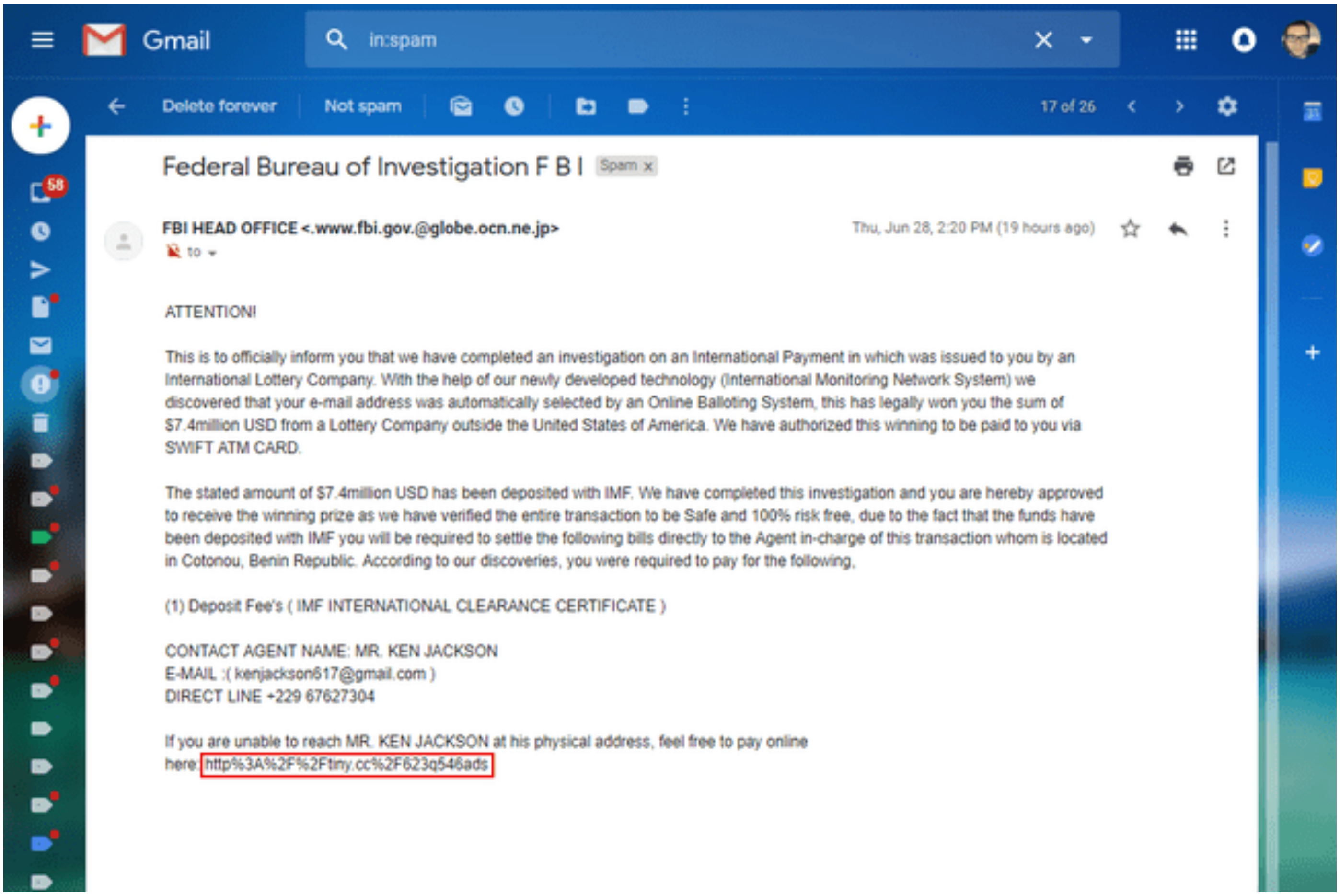
Note, I can successfully achieve this transfer within the shortest time from now if only you can offer your maximum cooperation to instruction and requirements, therefore your day to day correspondence is practically important.

Get back to me quickly

Beware of Links With Strange Character Strings

Some malware distributors conceal the destination of malware or phishing sites by using what is known as URL encoding. For example, with URL encoding, the letter *A* translates to *%41*.

Using encoding, malware distributors can mask destinations, commands, and other nasty stuff within a link so that you can't read it. Use a URL decoding tool, such as URL Decoder, to figure out the exact URL destination. (Visit the URL Decoder website for more information.)



Federal Bureau of Investigation F B I

FBI HEAD OFFICE <.www.fbi.gov.@globe.ocn.ne.jp>

Thu, Jun 28, 2:20 PM (19 hours ago)

ATTENTION!

This is to officially inform you that we have completed an investigation on an International Payment in which was issued to you by an International Lottery Company. With the help of our newly developed technology (International Monitoring Network System) we discovered that your e-mail address was automatically selected by an Online Balloting System, this has legally won you the sum of $7.4million USD from a Lottery Company outside the United States of America. We have authorized this winning to be paid to you via SWIFT ATM CARD.

The stated amount of $7.4million USD has been deposited with IMF. We have completed this investigation and you are hereby approved to receive the winning prize as we have verified the entire transaction to be Safe and 100% risk free, due to the fact that the funds have been deposited with IMF you will be required to settle the following bills directly to the Agent in-charge of this transaction whom is located in Cotonou, Benin Republic. According to our discoveries, you were required to pay for the following,

(1) Deposit Fee's (IMF INTERNATIONAL CLEARANCE CERTIFICATE)

CONTACT AGENT NAME: MR. KEN JACKSON
E-MAIL :(kenjackson617@gmail.com)
DIRECT LINE +229 67627304

If you are unable to reach MR. KEN JACKSON at his physical address, feel free to pay online here: http%3A%2F%2Ftiny.cc%2F623q546ads

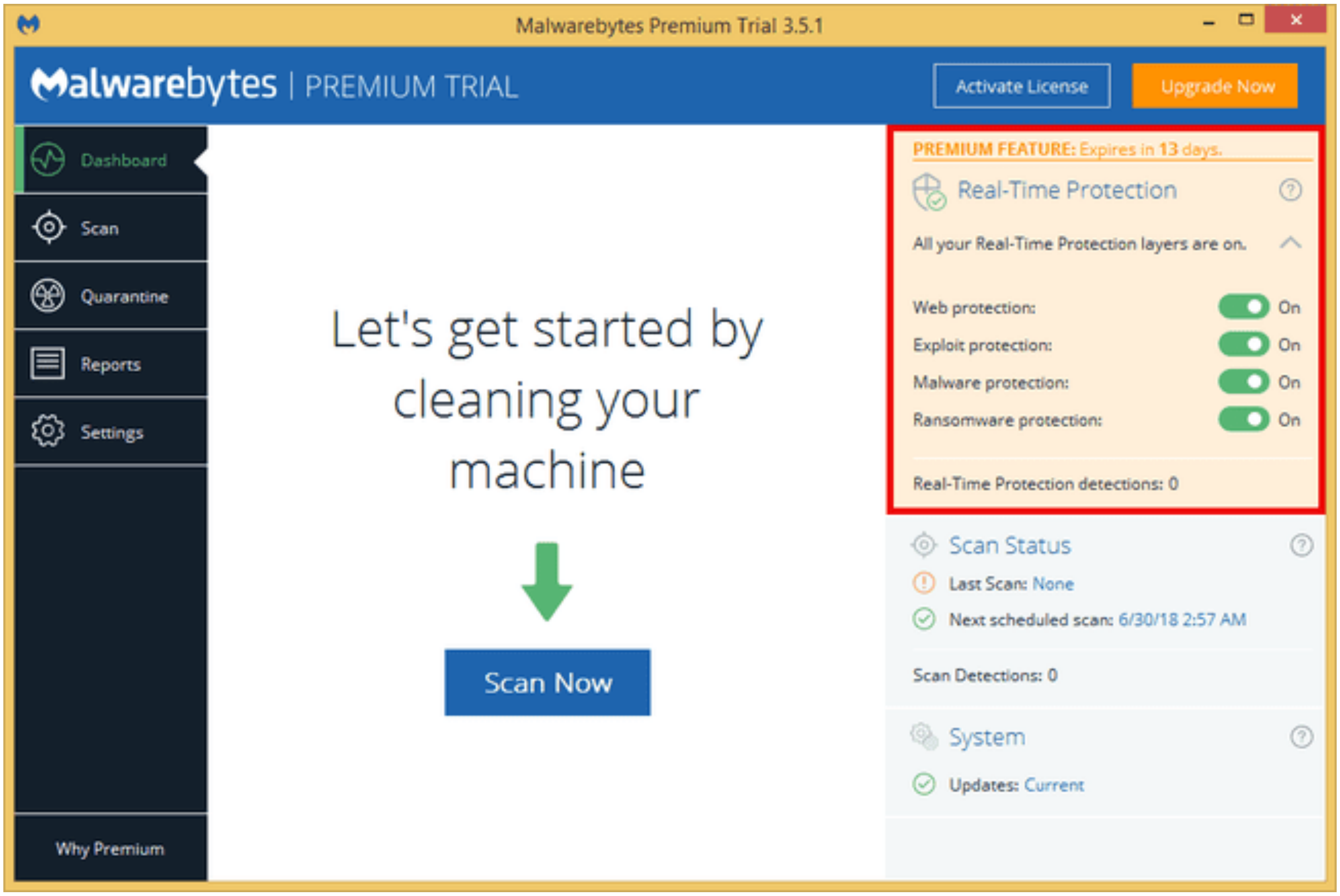
General Link Safety Tips

Scan the Link With a Link Scanner

Link scanners are websites and plug-ins that let you enter the URL of a suspicious link and check it for safety. Visit the Norton SafeWeb website, the URLVoid website, and the ScanURL website to learn about these products' link safety-checking capabilities. They index the remote destination and then report what was found so you never have to load the site on your own computer.

Enable Real-Time or Active Scanning in Anti-Malware Software

Take advantage of any active or real-time scanning options provided by your anti-malware software. These options may use more system resources, but it's better to catch malware while it's trying to enter your system rather than after your computer has already been infected.


Malwarebytes Premium Trial 3.5.1
Malwarebytes | PREMIUM TRIAL
Activate License
Upgrade Now
Dashboard
Scan
Quarantine
Reports
Settings
Why Premium
Let's get started by cleaning your machine
Scan Now

PREMIUM FEATURE: Expires in 13 days.

Real-Time Protection

All your Real-Time Protection layers are on.

Web protection: On
Exploit protection: On
Malware protection: On
Ransomware protection: On

Real-Time Protection detections: 0

Scan Status

Last Scan: None
Next scheduled scan: 6/30/18 2:57 AM

Scan Detections: 0

System

Updates: Current

Keep Your Anti-Malware and Antivirus Software Up to Date

If your anti-malware or antivirus software doesn't access the latest virus definitions, it's can't catch the latest threats in the wild that might infect your machine. Make sure your software is set to auto-update on a regular basis and check the date of its last update to ensure that updates are actually taking place.

Consider Adding a Second-Opinion Malware Scanner

A second-opinion malware scanner can offer a second line of defense should your primary antivirus fail to detect a threat. Some excellent second-opinion scanners, such as Malwarebytes and Hitman Pro, can make a real difference.