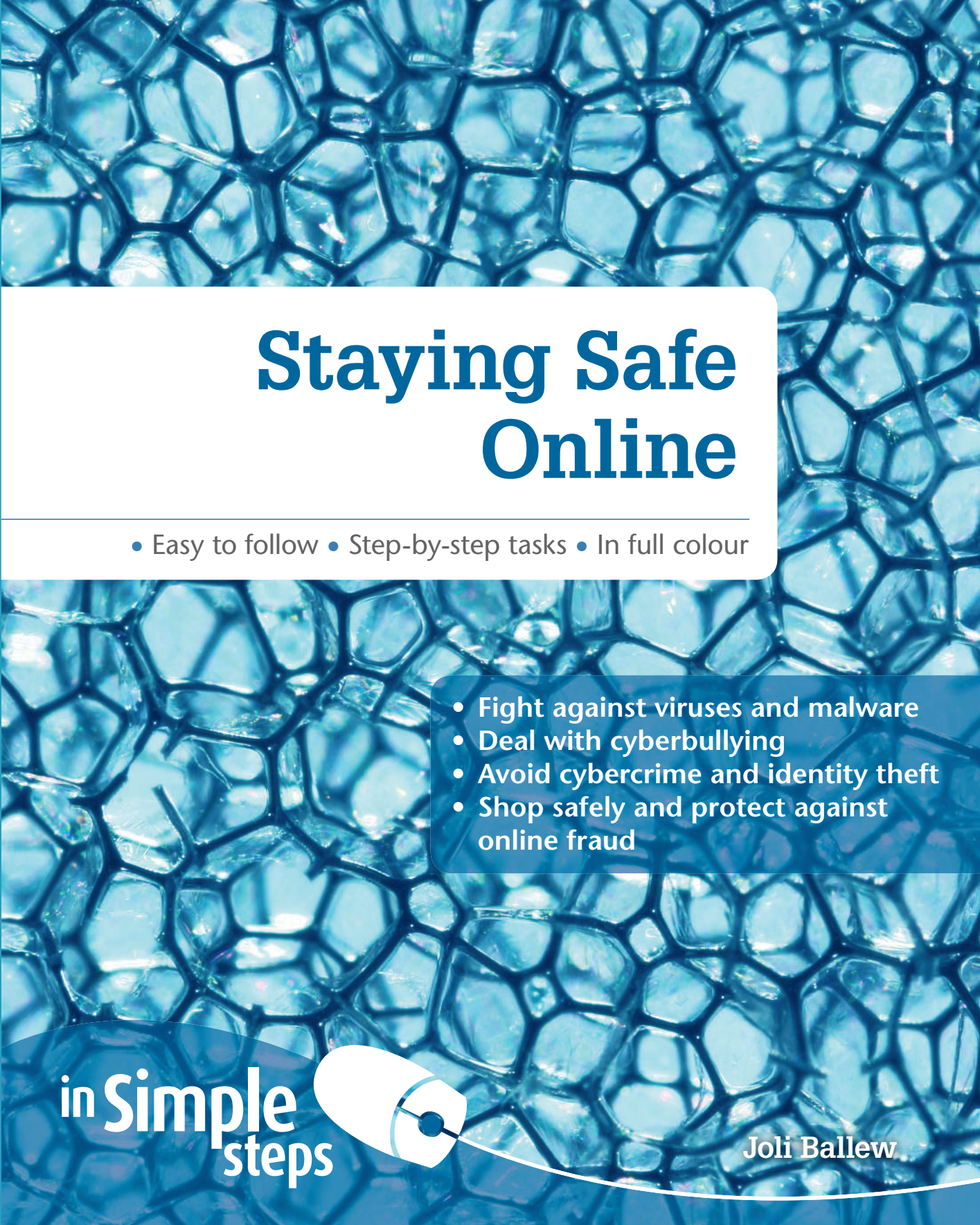


Staying Safe Online

• Easy to follow • Step-by-step tasks • In full colour

- Fight against viruses and malware
- Deal with cyberbullying
- Avoid cybercrime and identity theft
- Shop safely and protect against online fraud

in Simple steps

Joli Ballew

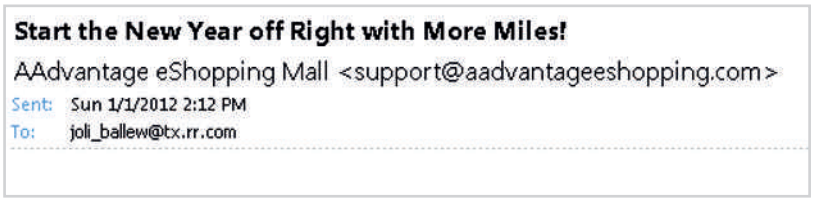
Staying Safe Online

PEARSON

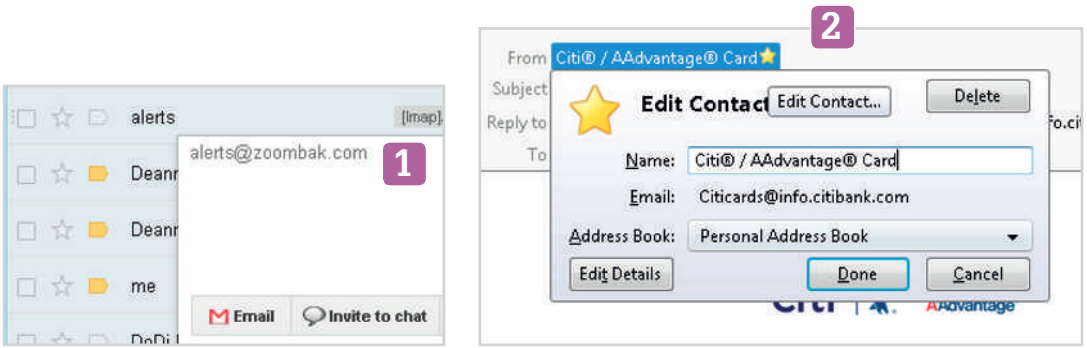
Harlow, England • London • New York • Boston • San Francisco • Toronto • Sydney • Auckland • Singapore • Hong Kong
Tokyo • Seoul • Taipei • New Delhi • Cape Town • São Paulo • Mexico City • Madrid • Amsterdam • Munich • Paris • Milan

Explore the validity of the sender's name

Some senders mask the name that appears in the From: line to make the email appear as though it's from a valid source, when in reality it is not. In many email programs and browsers, the actual email address appears next to the name, as shown here. This is good, because you can tell if the email address matches the sender's name and is one you recognise. If you can't see the email address but can only see the name instead, don't do anything with the email until you're sure you know who it is from.



1. If you get your email from a web browser, by navigating to a web page, you may be able to see the actual email address by hovering your mouse over the name.
2. If you get your email from a program installed on your computer, hovering will probably work there too. If not, click once on the sender's name.



HOT TIP: You can often right-click the email address in the To: line to view additional options, like Properties or Edit.

ALERT: If the email is supposed to be from, say, CitiBank, but the email address is something like CD43Dclies450@mywebaddress.com, it's not legitimate.

Hover before you click that link

It's easy for someone to create a link in an email where the name of the link is different from the actual website you'll be taken to if you click it. This means that a link's name could be the name of a legitimate company, but the website it is pointing to is something completely different. Before clicking any link, hover the mouse over it to see where the link actually goes.

1. Open any email that contains a link to a web page.
2. Hover your mouse over the link.
3. Verify that the words after *www* represents the site you really want to go to.
4. Click the link only if you know the website link is a valid one. Better yet, navigate to the site yourself, as outlined in the next section.

ALERT: When in doubt about a link, don't click it.

ALERT: If you want to click a link for a bank, company or well-known online site (like Microsoft or Apple), note that the words after *www* should contain the company name (www.microsoft.com, for instance). It's okay if something else follows those words though (www.microsoft.com/security).

When in doubt, visit the entity's official website

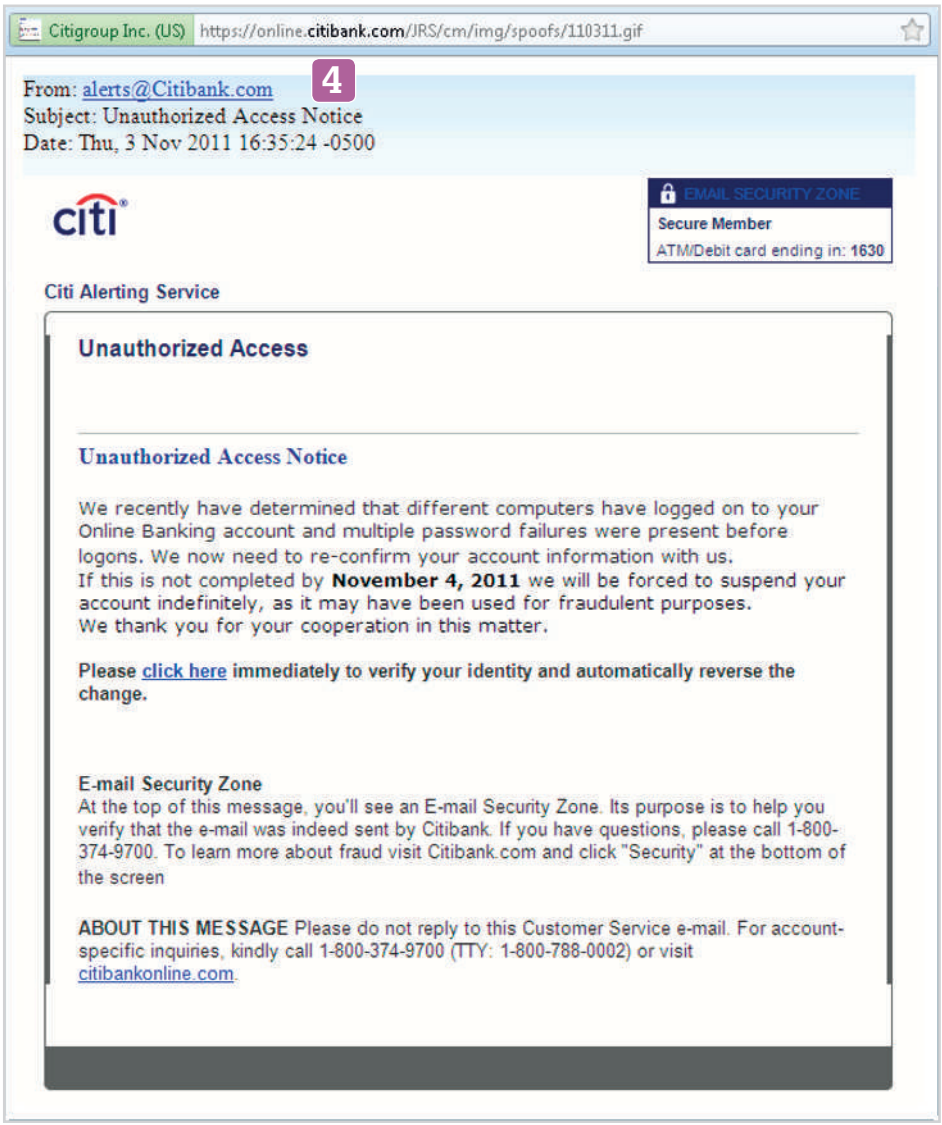
If you receive an email from a company you trust and/or have an account with, and you receive an email that asks you to reply with your personal information for 'verification' or some such thing, and you can't tell from the sender's email address or any links in the body of the email if it is a scam, you still have options. You can visit the website by typing in the address manually, and look there for information.

1. Open your web browser. This may be Safari, Firefox or Internet Explorer, for instance.
2. In the address bar, type the name of the website you'd like to visit.
3. Look around the site for a Security tab or a Help tab.

DID YOU KNOW?

If a company, like a financial institution, needs you to update your personal information, you'll be prompted to do so when you log on to the website. You will never be asked to provide that information in an email. It's just not secure.

4 Locate information about recent email scams. Here is an example of a scam email. This email is *not* from Citibank!


Citigroup Inc. (US) https://online.citibank.com/JRS/cm/img/spoofs/110311.gif

From: alerts@Citibank.com 4
Subject: Unauthorized Access Notice
Date: Thu, 3 Nov 2011 16:35:24 -0500

citi

EMAIL SECURITY ZONE
Secure Member
ATM/Debit card ending in: 1630

Citi Alerting Service

Unauthorized Access

Unauthorized Access Notice

We recently have determined that different computers have logged on to your Online Banking account and multiple password failures were present before logons. We now need to re-confirm your account information with us.
If this is not completed by **November 4, 2011** we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.
We thank you for your cooperation in this matter.

Please click here immediately to verify your identity and automatically reverse the change.

E-mail Security Zone
At the top of this message, you'll see an E-mail Security Zone. Its purpose is to help you verify that the e-mail was indeed sent by Citibank. If you have questions, please call 1-800-374-9700. To learn more about fraud visit Citibank.com and click "Security" at the bottom of the screen

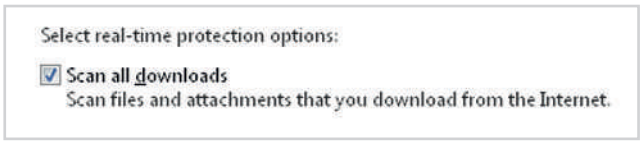
ABOUT THIS MESSAGE Please do not reply to this Customer Service e-mail. For account-specific inquiries, kindly call 1-800-374-9700 (TTY: 1-800-788-0002) or visit citibankonline.com.

HOT TIP: Always hover the mouse or click the sender's address to see who it's from.

ALERT: Always hover the mouse over a link before clicking it. If the link claims to go to www.citi.com but instead goes to www.123x7z.ripyouoff.com, don't click it.

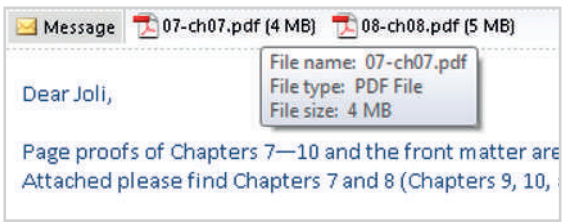
Triple check before opening an attachment

You already know that attachments that come with emails can contain viruses and other problematic computer code. And since viruses can replicate themselves and spread through email, it's possible to get a virus from an email sent by someone you know. First and foremost, make sure your security software is set to scan all attachments, as shown here.



Then, review these additional tips to stay safe.

- Understand that it's perfectly OK to reply to the sender and ask if they meant to send the email attachment, and if they believe it's safe to open.
- Hover your mouse over the attachment to see what kind of file it is. It's safe to open PDF files, pictures and most documents, but don't open anything that is an EXE, BAT, COM, PIF or SCR.



- Beware of files that have an 'm' in their name, like .docm, .xlsm and so on. These are office files that contain macros. Macros are computer code, and can be unsafe.

DID YOU KNOW?

The name of the attachment may appear to be safe, such as *pictureofme.jpg*, but when you hover over it, you may find it's really *pictureofme.jpg.exe*. Clicking that would be bad indeed!

WHAT DOES THIS MEAN?

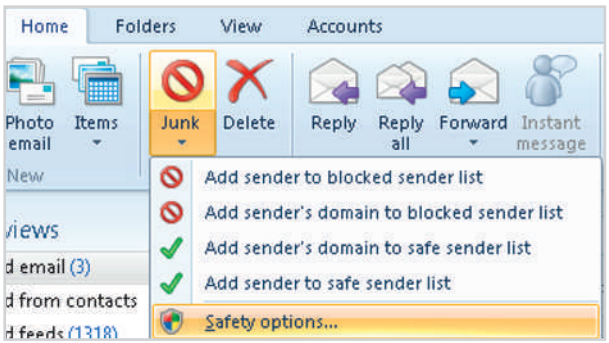
.exe: files that end in .exe are executable files, and clicking them causes a program installation to begin.

HOT TIP: You can configure security software to scan attachments for viruses before they are opened.

Configure a junk email filter

If you keep junk mail from getting into your inbox, you'll certainly be much less likely to fall for a scam you see there. Thus, one of the ways to protect yourself is to set a junk email filter. How you go about this depends how you get your email.

- If you use Microsoft Outlook, from the Home tab, click the arrow under Junk, and click Junk E-Mail options to configure settings.
- If you use Mozilla Thunderbird, click Tools, Options and the Junk tab.
- If you use Windows Live Mail, from the Home tab, click the arrow under Junk, and click Safety Options, as shown here.



- If you use Apple Mail, go to Mail, Preferences and then Junk Mail.
- If you use a web-based method then visit the web page where you get your email, and search for junk mail filtering options.

DID YOU KNOW?

If you check your email from a website, like www.gmail.com or www.hotmail.com, junk email filtering is built-in, but you can often edit the settings.

DID YOU KNOW?

If you configure your junk email options to the most restrictive (highest security) option, you'll probably send a lot of valid email to the Spam or Junk folder.

HOT TIP: No matter what junk or spam setting you select, you may still find valid email in the Spam or Junk folder. Check these folders occasionally just to be sure, but never pull email from them until they are from a contact you know.