7 forms of fraud, popular online fraud

Anyone who has used the Internet knows that you can't trust everything online. Because something seems credible doesn't mean it's exactly what it says.

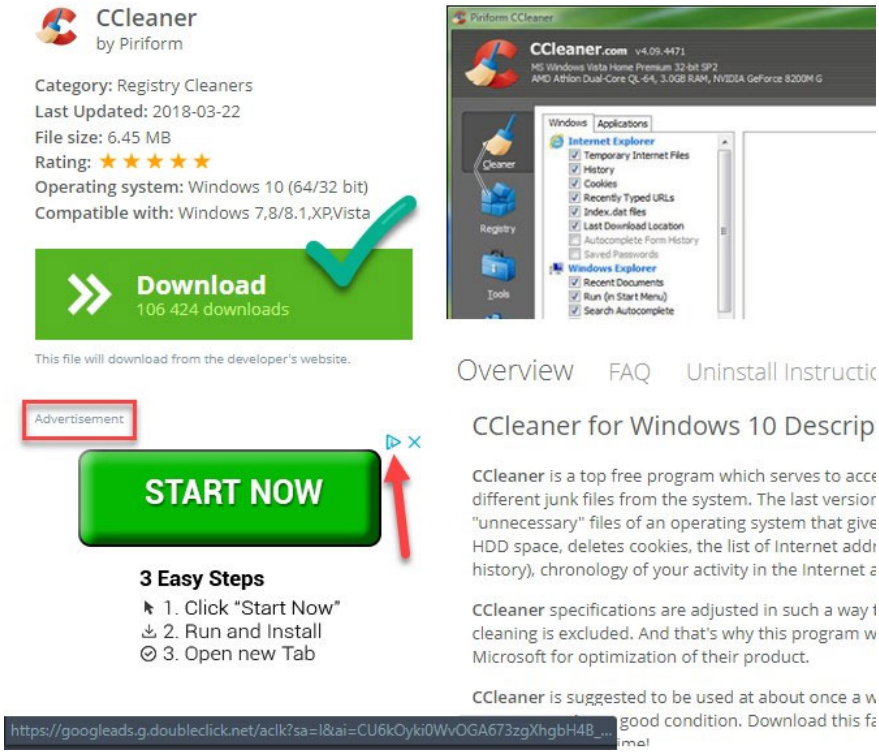
Anyone who has used the Internet knows that you can't trust everything online. Because something seems credible doesn't mean it's exactly what it says.

Knowing how to detect fake content online is an important skill to avoid wasting time, money or destroying your property. Here are 7 commonly faked online content and some tips to discover them.

Types of phishing and phishing online

1. 1. Fake download button
2. 2. Email scam
3. 3. Notice of fake updates
4. 4. Fake reviews and reviews
5. 5. Fake website
6. 6. Social network fraud
7. 7. Fake images

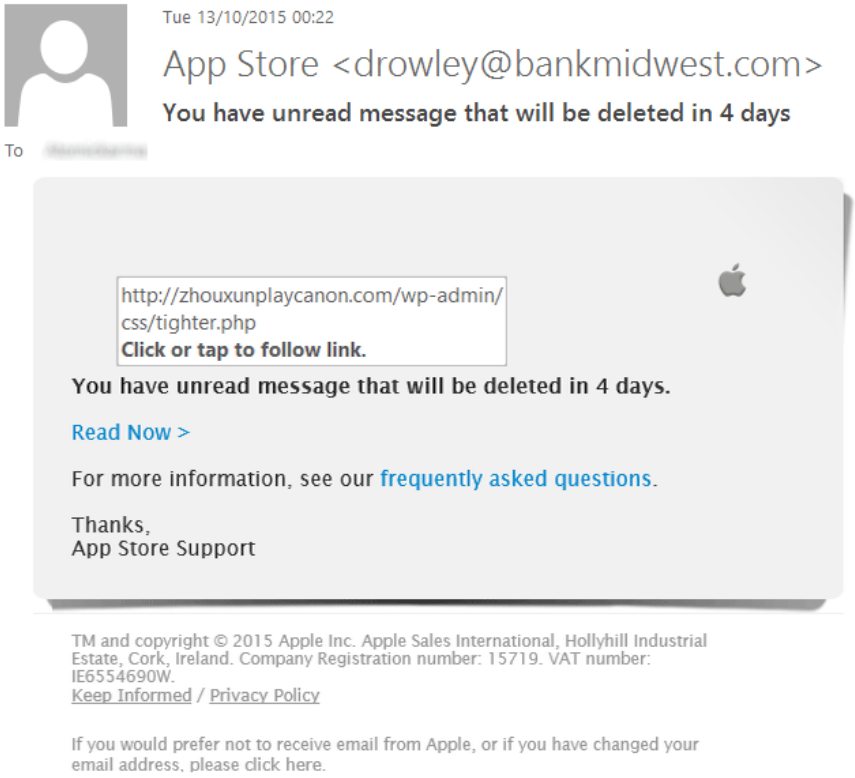
1. Fake download button



Fake links appear on all websites through Google's AdSense ads because scammers constantly push them to the site. Even worse when they appear on the page you are looking for in the legal file, software downloads.

When you click on this Download fake button, you will download useless or dangerous software. Read the article Tips to avoid fake Download button to know how to avoid these fake download links.

2. Email scam



What about spam emails that are easily detected but phishing emails that want to steal personal information or trick you into downloading malware? Usually they are like real emails from friends or trusted partners like banks.

You need to keep in mind some rules when determining whether an email is real or not.

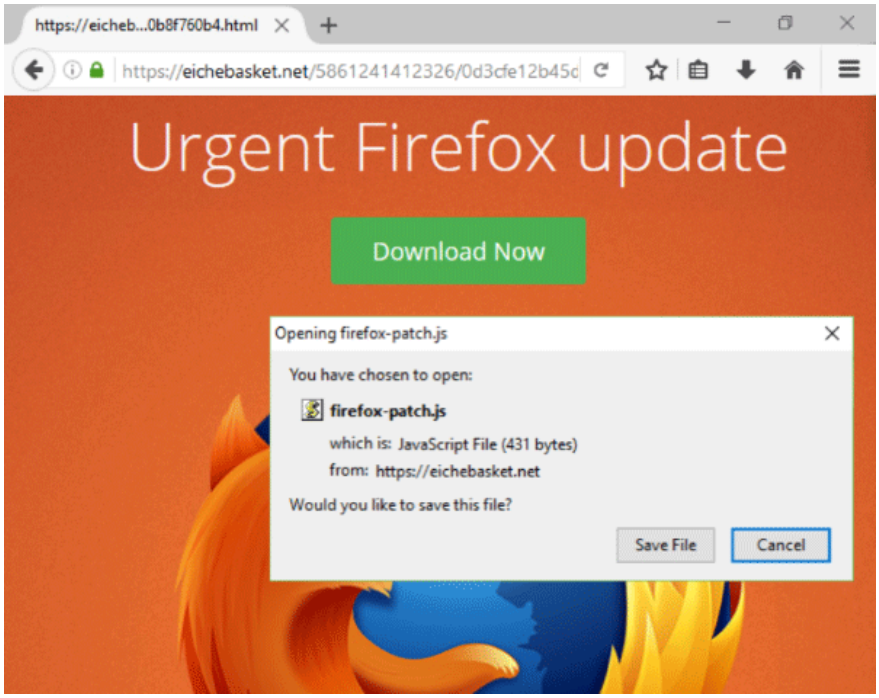
First, you should check the sender. Although it is possible to fake a message and make it look like it came from a trusted email address, it is common for fake emails to come from a fake address. If you see the official messages coming from @ paypal.com address and email from @ paypalservicealerts.com, you know there is a problem. This also applies to emails coming from your contacts.

You should also consider the content of the message to see if it is fake. Legitimate companies do not require credit card information, social insurance numbers, passwords or other sensitive information via email. Phishing emails are often created to make you quickly click.

Like checking the Download button, you can hover over the link in the email to see its address. An official email will lead to the official website. If you see a strange site name, do not click on it.

In general, if you receive an email that you are unsure of, visit the site directly and check. If PayPal needs you to verify something, you will see it when logging in.

3. Notice of fake updates

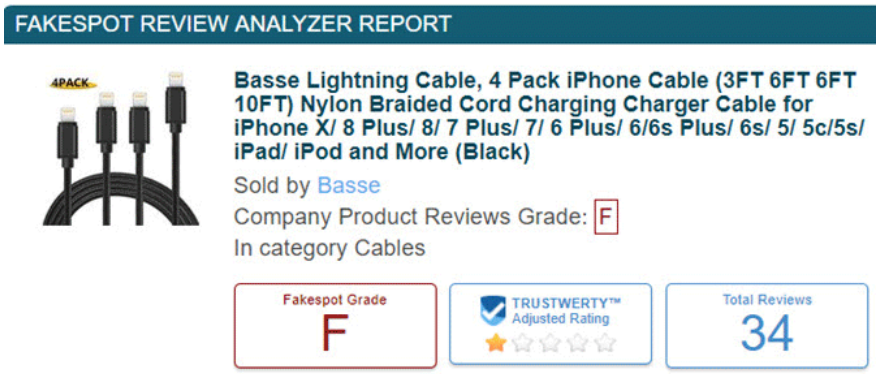


Some applications automatically update, but others will notify users of manual updates. So some ads took advantage of this point and disguised themselves as a prompt to update fake.

If you see a message when you are online asking to install an 'recommended' update for Java, Flash or other plugins, you should not click on it. The program does not use random pop-up windows from the website to notify users of updates. The software update notice appears when the computer first starts up, most of them are safe unless you have adware.

Like phishing emails, you must always open the mentioned software and check for manual updates. Nearly all applications have their own update checker in **Help> Check for Updates** or similar.

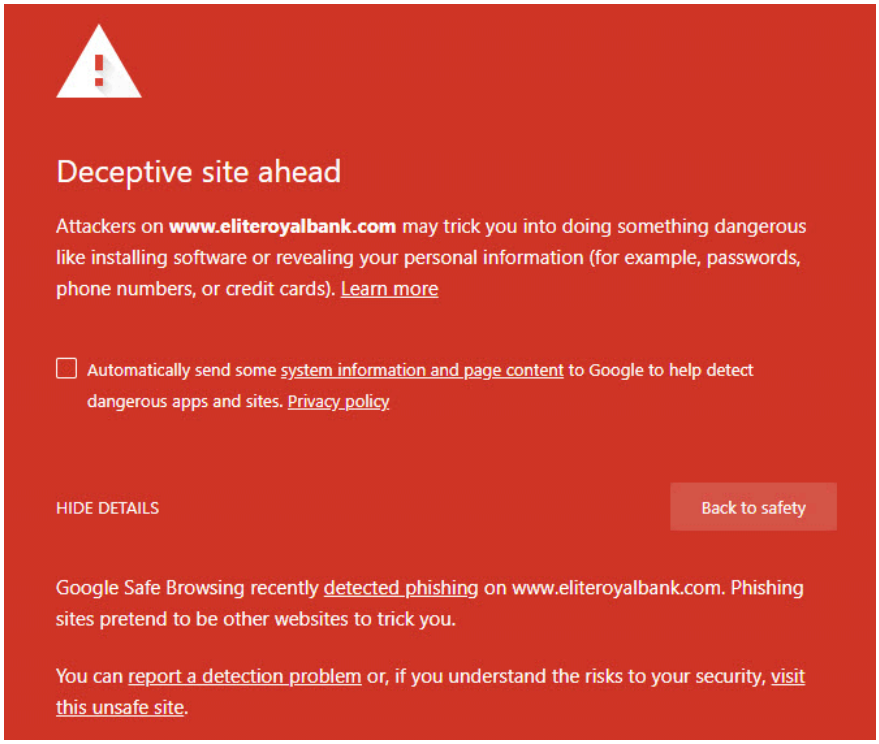
4. Fake reviews and reviews



Judging from previous user experience helps you decide whether to buy or use the product. However, it is not surprising that these reviews are fake to increase the reputation of a fake item. So you should not blindly trust the reviews on shopping sites.

You can detect fake reviews by checking the excessive use of keywords, unnatural language and vague compliments.

5. Fake website



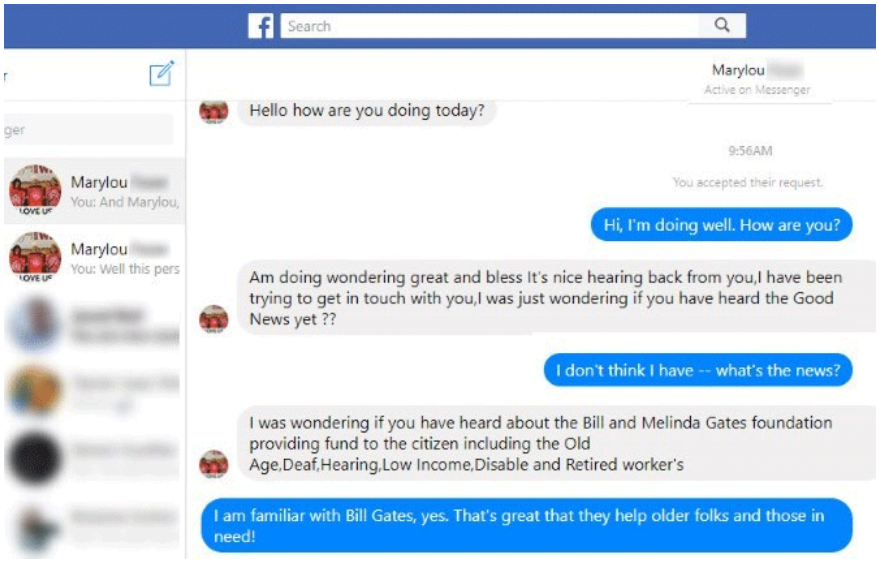
Fake websites are often linked to the fake email above. If the scammers make you click on an email or follow an ad, you will be taken to a fake camouflage site that makes you trust.

The most important way to avoid becoming a victim of these fake websites is to check the URL. Although phishers can create sites that look 'similar' to the real site, they cannot use the actual URL. These sites often have one or more of the following identifiers in the URL.

1. There are many dashes (best-online-deals-everyday.com)
2. Use numbers or symbols instead of letters (paypa1.com, 0nlinebonk.com)
3. Extension of unusual domain names like .biz.
4. Domain name fraud. You need to remember that the string before the extension (.com) is the real name of the website. Fake websites use addresses like paypal.fakesite.com and banking.fakesite.com.

See contact information and copyright at the bottom of the page. If this information is vague, unclear, or misspelled in the old copyright or copyright statement, these are fake websites.

6. Social network fraud



On social networking sites, especially Facebook, you should be careful with those who create fake profiles with your real friends' information. Scammers often steal someone's avatar and create an account with their name. Then will text that person's friend to ask for money or provide a link to the phishing site.

To avoid this, you should message your friends via a trust channel (like calling) if you receive a strange message from them. If you see a friend request from someone and you are their friend, that could be a fake.

7. Fake images

Thanks to Photoshop and everyone can share anything, hoaxing images have become popular for a long time. With today's more powerful image editing tools, it's hard to know if something is real or edited.

Often, images of text spread on social media, claiming old legends like Facebook will start charging. Unless you are a Photoshop expert or the image has an obvious mistake, you will not be able to discover it yourself. Try using a tool like FotoForensics to analyze images.

Searching for images backwards on Google is also a good way to learn more about them. If you search for an image and it gives countless articles about a hoax, you'll know it's not real.

Now you know some common phishing and phishing forms. Although, it can be difficult to distinguish real web pages, emails and images from cleverly disguised counterfeit goods. But using these tips, you will be able to see through the lies more easily and the rest will be based on your experience.