7 Signs to identify Phishing Emails

2019-09-12 - Don Guilbeault - Comments (0) - General

What is phishing?

Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information. This is usually done by including a link that will appear to take you to the company's website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam.

The term 'phishing' is a spin on the word fishing, because criminals are dangling a fake 'lure' (the email that looks legitimate, as well as the website that looks legitimate) hoping users will 'bite' by providing the information the criminals have requested – such as credit card numbers, account numbers, passwords, usernames, and more.

Phishing emails today rarely begin with, *"Salutations from the son of the deposed prince of Nigeria..."* It's often difficult to distinguish a fake email from a verified one, however most have subtle hints of their scam nature. Are you sure that email from UPS is actually from UPS? (Or Costco, Best Buy, or the myriad of unsolicited emails you receive every day?) Companies and individuals are often targeted by cyber-criminals via emails designed to look like they came from a legitimate bank, government agency, or organization. In these emails, the sender asks recipients to click on a link that takes them to a page where they will confirm personal data, account information, etc. Here are seven email phishing tips to help you recognize a malicious email and maintain email security.

1. Legit companies don't request your sensitive information via email

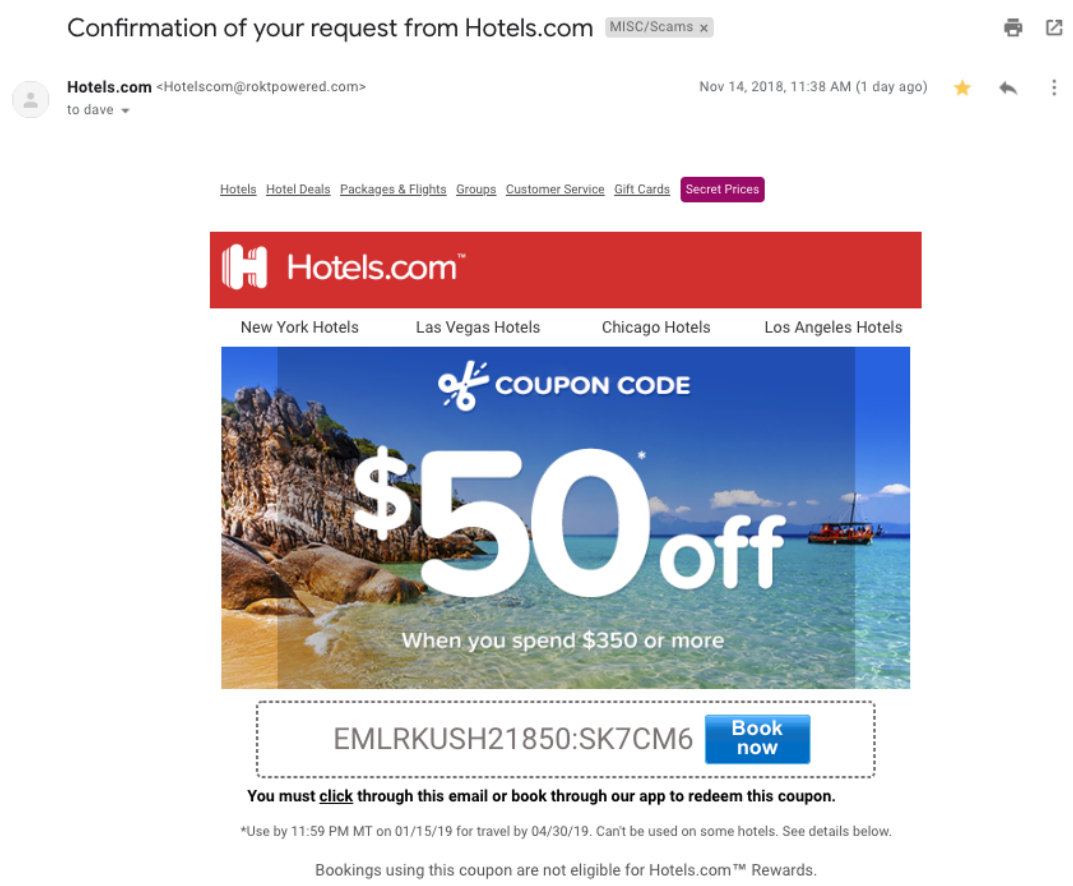
Chances are if you receive an unsolicited email from an institution that provides a link or attachment and asks you to provide sensitive information, it's a scam. Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.

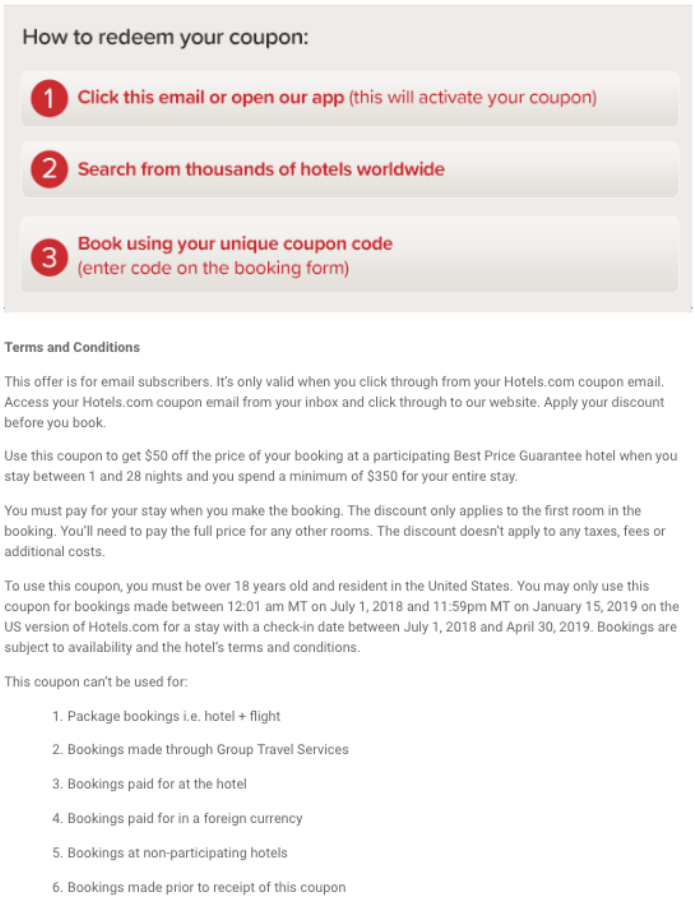
2. Legit companies usually call you by your name

Phishing emails typically use generic salutations such as "Dear valued member," "Dear account holder," or "Dear customer." If a company you deal with required information about your account, the email would call you by name and probably direct you to contact them via phone. **BUT**, some hackers simply avoid the salutation altogether. This is

especially common with advertisements.

The phishing email below is an excellent example. Everything in it is nearly perfect. So, how would you spot it as potentially malicious?





How to redeem your coupon:

1. **Click this email or open our app** (this will activate your coupon)
2. **Search from thousands of hotels worldwide**
3. **Book using your unique coupon code** (enter code on the booking form)

Terms and Conditions

This offer is for email subscribers. It's only valid when you click through from your Hotels.com coupon email. Access your Hotels.com coupon email from your inbox and click through to our website. Apply your discount before you book.

Use this coupon to get $50 off the price of your booking at a participating Best Price Guarantee hotel when you stay between 1 and 28 nights and you spend a minimum of $350 for your entire stay.

You must pay for your stay when you make the booking. The discount only applies to the first room in the booking. You'll need to pay the full price for any other rooms. The discount doesn't apply to any taxes, fees or additional costs.

To use this coupon, you must be over 18 years old and resident in the United States. You may only use this coupon for bookings made between 12:01 am MT on July 1, 2018 and 11:59pm MT on January 15, 2019 on the US version of Hotels.com for a stay with a check-in date between July 1, 2018 and April 30, 2019. Bookings are subject to availability and the hotel's terms and conditions.

This coupon can't be used for:

1. Package bookings i.e. hotel + flight
2. Bookings made through Group Travel Services
3. Bookings paid for at the hotel
4. Bookings paid for in a foreign currency
5. Bookings at non-participating hotels
6. Bookings made prior to receipt of this coupon

This is a very convincing email. For me, the clue was in the email address domain. More on that below.

3. Legit companies have domain emails

Don't just check the name of the person sending you the email. Check their email address by hovering your mouse over the 'from' address. Make sure no alterations (like additional numbers or letters) have been made. Check out the difference between these two email addresses as an example of altered emails: *michelle@paypal.com vs michelle@paypal23.com* Just remember, this isn't a foolproof method. Sometimes companies make use of unique or varied domains to send emails, and some smaller companies use third party email providers.

4. Legit companies know how to spell and use grammar

Possibly the easiest way to recognize a scam email is bad grammar. An email from a legitimate organization should be well written. Little known fact – there's actually a purpose behind bad syntax. Hackers generally aren't stupid. They prey on fears of the individual by Capitalizing and **bolding** key words that your eyes are drawn to when you are quickly skimming through an email.

5. Legit companies don't force you to their website

Sometimes phishing emails are coded entirely as a hyperlink. Therefore, clicking accidentally or deliberately anywhere in the email will open a fake web page, or download

malware onto your computer. Avoid click on the message body when possible.

6. Legit companies don’t send unsolicited attachments

Unsolicited emails that contain attachments reek of hackers. Typically, authentic institutions don’t randomly send you emails with attachments, but instead direct you to download documents or files on their own website.

This method isn’t foolproof. Sometimes companies that already have your email will send you information, such as a white paper, or flyer that may require a download. In that case, be on the lookout for high-risk attachment file types include **.exe**, **.scr**, and **.zip**. (When in doubt, contact the company directly using contact information obtained from their actual website.)

7. Legit company links match legitimate URLs

Just because a link says it’s going to send you to one place, doesn’t mean it’s going to. Double check URLs. If the link in the text isn't identical to the URL displayed as the cursor hovers over the link, that's a sure sign you will be taken to a site you don’t want to visit. If a hyperlink’s URL doesn’t seem correct, or doesn’t match the context of the email, don’t trust it. Ensure additional security by hovering your mouse over embedded links **(without clicking!)** and ensure the link begins with https:// and the URL aligns with the senders business website.

Hopefully now armed with the knowledge above you will be better equipped to identify and remove unwanted, unsolicited phishing emails from your mail box. Remember we all have to be responsible for our own activities online and **"When in doubt just DELETE"**. then contact the sender to resend the email if it is important.

Original Article by: David Ellis VP Investigations CISSP, QSA, PFI
https://tinyurl.com/y6h66l49

Integrity | Excellence | Responsibility | Community