



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?


Confirmation of your request from Hotels.com MISC/Scams x 🖨️ 🔗

 **Hotels.com** <Hotelscom@roktpowered.com> Nov 14, 2018, 11:38 AM (1 day ago) ★ ↩️ ⋮
to dave ▾

[Hotels](#) [Hotel Deals](#) [Packages & Flights](#) [Groups](#) [Customer Service](#) [Gift Cards](#) [Secret Prices](#)

 **Hotels.com™**

[New York Hotels](#) [Las Vegas Hotels](#) [Chicago Hotels](#) [Los Angeles Hotels](#)



EMLRKUSH21850:SK7CM6 [Book now](#)

You must click through this email or book through our app to redeem this coupon.

*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

Bookings using this coupon are not eligible for Hotels.com™ Rewards.