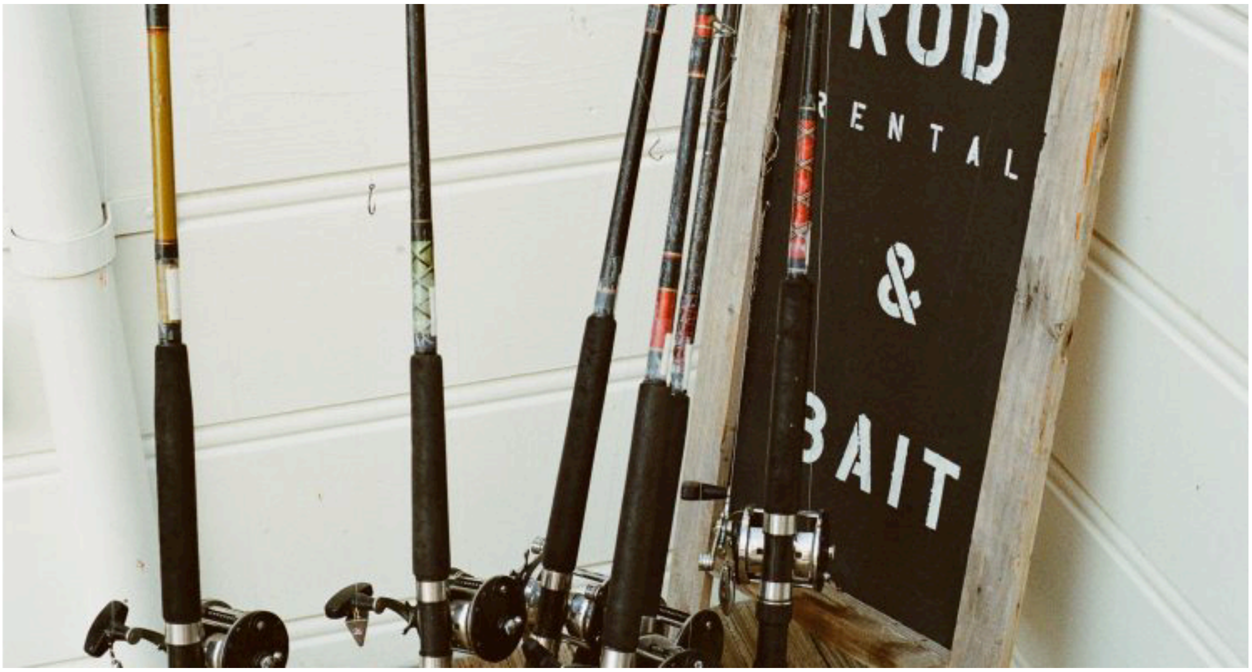


Gone phishing

May 31, 2017

Save yourself time, money and headaches by learning how to recognize and avoid malicious emails that fool you into giving up your personal information.

Consider this example: on May 24, 2017, the following email was sent to the personal email address of a staff person notifying them about a delivery from FedEx.

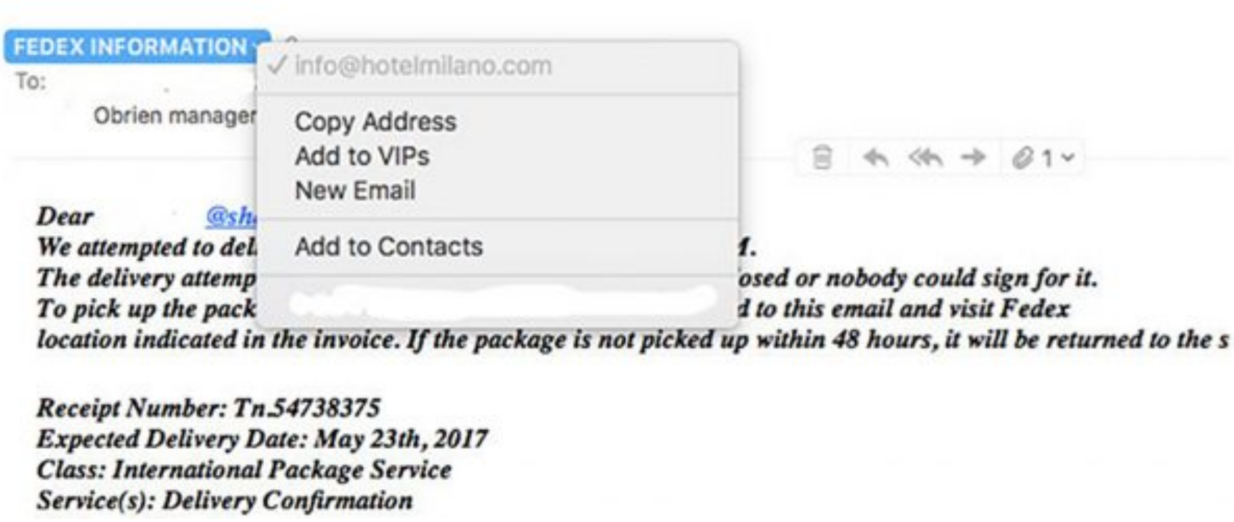
Dear ____
We attempted to deliver your item on May 23th, 2017, 09:30 AM. The delivery attempt failed because the address was business closed or nobody could sign for it. To pick up the package. Please, print the receipt that is attached to this email and visit Fedex location indicated in the invoice. If the package is not picked up within 48 hours, it will be returned to the sender.
Receipt Number: Tn. 54738375
Expected Delivery Date: May 23th, 2017-05-30
Class: International Package Service
Service(s): Delivery Confirmation
Status: Notification sent
Thank you

At first glance, it is reasonable to think a package has been sent and needs to be picked up, especially if your are anticipating a delivery. But on second look, the red flags common to phishing emails become apparent.

In the screen image below, you can see the blue *From*: box reads “FEDEX INFORMATION.”

But hover (not click) the mouse pointer over the name, the real address is revealed as “*info@hotelmilano.com.”*

The email is not from FedEx, nor does it appear to be from the person written at the bottom of the email – *R. Obrien*, supposedly a FedEx manager.



Dear @sh
We attempted to del 1.
The delivery attemp osed or nobody could sign for it.
To pick up the pack d to this email and visit Fedex
location indicated in the invoice. If the package is not picked up within 48 hours, it will be returned to the s

Receipt Number: Tn.54738375
Expected Delivery Date: May 23th, 2017
Class: International Package Service
Service(s): Delivery Confirmation

The mismatch between the sender's name and the actual email is all you need to know to determine this is a phishing email.

On further reading you may notice other details that are not right. The second sentence reads, "…..the address was business closed….nobody could sign for it," followed by an incomplete sentence – "To pick up the package."

It is English but the grammar and usage are incorrect, which is very typical of a phishing email. (Note: Some phishing emails are well-written so there are no absolutes.)

This email has another feature common to phishing mail. It contains a warning to induce the reader to act "…*within 48 hours*…" before the package is returned.

Another test of an email's legitimacy is whether it makes it through your anti-malware software. In this particular case, the email was blocked from entering the staff person's email accounts.

Watch for these other giveaways such as emails that:

- Ask you to update, confirm or validate your account
- Make threats of account closures or other negative consequences if you don't act
- Tout great bargains or special offers that sound too good to be true
- Come from a charitable organization requesting donations following a disaster or tragedy in the headlines

If you receive a suspicious email from a financial institution or credit card company with an attachment, or with a hyperlink, you should definitely not click on it as it may lead you to a fraudulent website.

What to do if your personal information may have been compromised

If you realize you've made a mistake of submitting information through an email such as account numbers or passwords, call your bank and or credit card company using telephone numbers from a directory or a bill (not from the email!) and notify them. They will place your account on hold until the matter is cleared.

If a criminal has hacked into your email and used your identity and email address to send a phishing scam to another person, you should contact everyone with whom you are dealing with in a large transaction, and alert them of a potential fraud.

The most effective prevention is to secure your email and other digital accounts with secure passwords.

Here are some password tips:

1 Always keep your password secret.
2 Create passwords that are nearly impossible for someone to guess, or for a hacker's software to decode, but which you can remember without writing down.
3 Avoid passwords that comprise a stew of various numbers, letters and symbols, which are difficult for most of us to remember. Instead, choose a theme or a subject that you can update and also recall.
4 Do not use usernames or passwords that are easy to guess such as "password" or "admin".
5 Set up "two-factor authentication" (2FA) or "two-step verification" so that in addition to a username and password you have a second level of security such as a PIN number, code, another password, even a fingerprint which is unique to you. Then if anyone else tries to sign in to your account from *another computer*, they won't be permitted to do so without your code.

2FA is available in Google mail, Facebook and apps such as Outlook.

However you must set it up yourself by logging on to your webmail account and looking for the preferences or security section of the site. There will be some technical requirements you need to check. The alternative is to purchase a security key from a tech retailer that will plug into the USB port of your computer and prevent other users from logging on.