Cashless Payment and Security Part 2

IT news this week will be a continuation of the previous topic, cashless security.

Before we start, however, let me highlight one other benefit of purchasing through QR code over a credit card. This benefit is with the speed of notifications.

Any purchases done through a QR code would send an email or text notifying the user of the purchase, letting them know immediately if there was anything wrong.

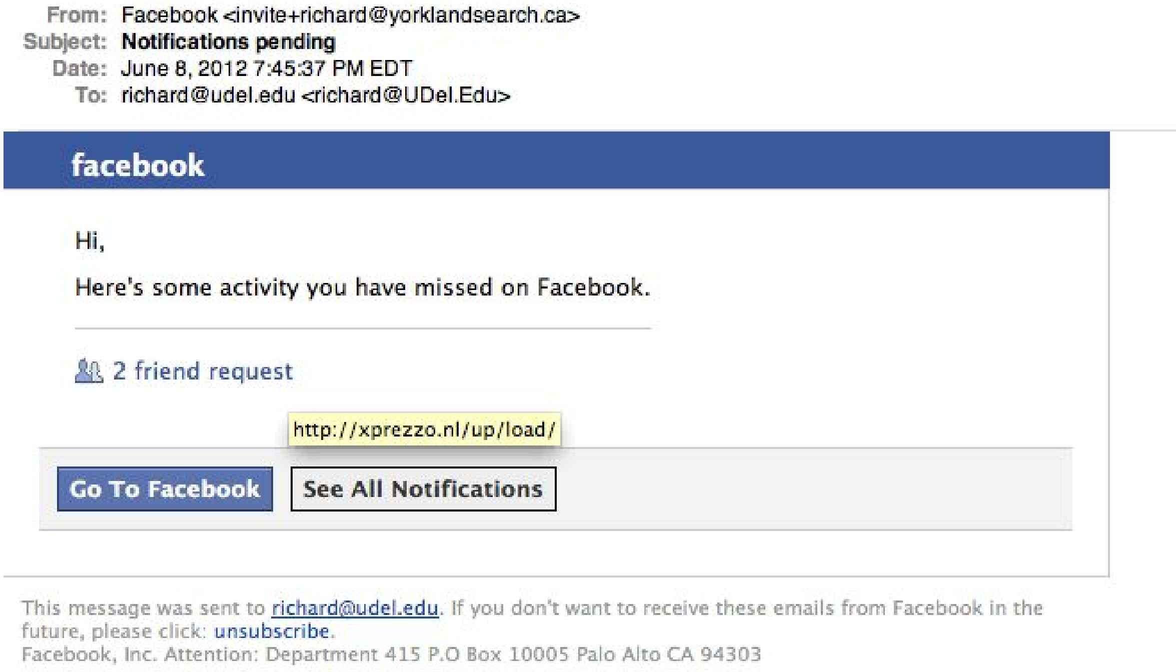
Though reassuring, since the number of emails received increases, one has to be careful of another risk, phishing scam.

Phishing is not an act of fishing, it is an act of sending an email disguised as a financial institution and fraudulently collecting personal information such as user ID, password, address, name, bank account number, credit card number, etc. This triggering email is called phishing email and the connected site is called phishing site.

What is Phishing?

What does a phishing email look like? These are two examples of common phishing emails.

Do they seem suspicious to you?



From: Facebook <invite+richard@yorklandsearch.ca>
Subject: **Notifications pending**
Date: June 8, 2012 7:45:37 PM EDT
To: richard@udel.edu <richard@UDel.Edu>

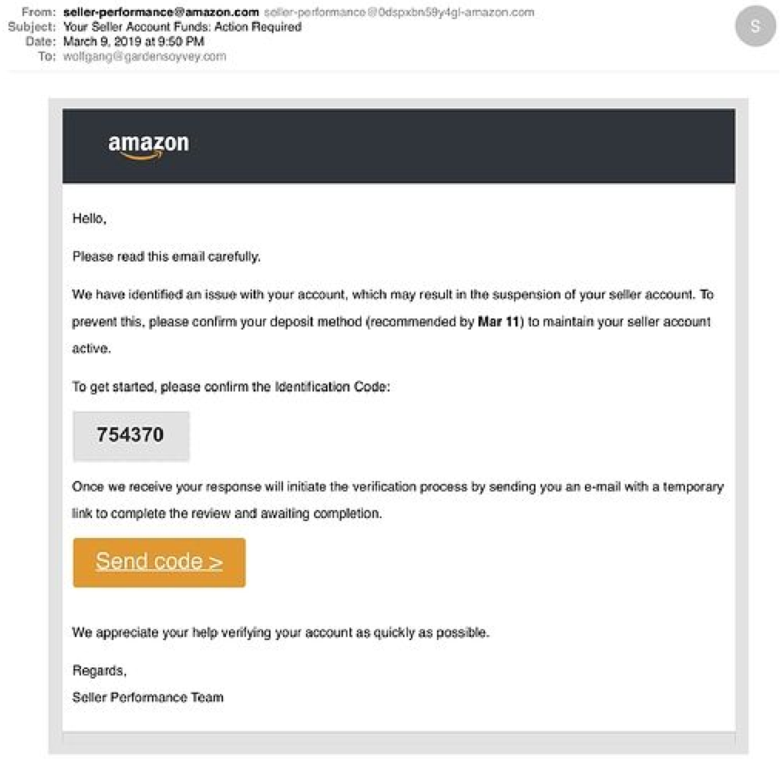
Hi,

Here's some activity you have missed on Facebook.

2 friend request

http://xprezzo.nl/up/load/

This message was sent to richard@udel.edu. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303



From: **seller-performance@amazon.com** seller-performance@0dspxbn59y4gl-amazon.com
Subject: Your Seller Account Funds: Action Required
Date: March 9, 2019 at 9:50 PM
To: wolfgang@gardensoyvey.com

Hello,

Please read this email carefully.

We have identified an issue with your account, which may result in the suspension of your seller account. To prevent this, please confirm your deposit method (recommended by **Mar 11**) to maintain your seller account active.

To get started, please confirm the Identification Code:

754370

Once we receive your response will initiate the verification process by sending you an e-mail with a temporary link to complete the review and awaiting completion.

We appreciate your help verifying your account as quickly as possible.

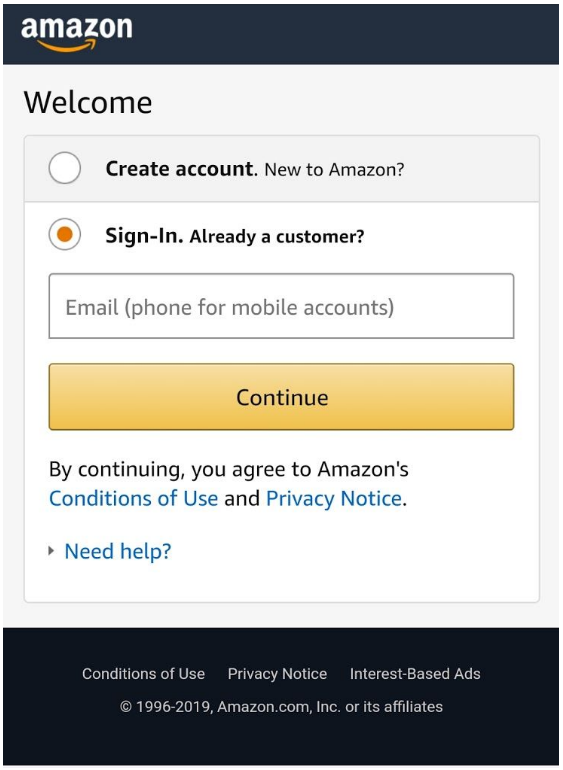
Regards,
Seller Performance Team

Previously, it was said to be careful of emails with bad English grammar. That is still true today, however, now we have to be careful of emails with good English as well. Some phishing emails would copy directly from the original email, which may make it difficult to see at first glance.

There is also an increasing number of cases where a message is being sent through text, and since the text messages are generally short, it may be harder to notice.

Recently, there has been an increasing number of companies using SMS for two-factor authentication and confirmation of delivery status. So it may come naturally for some to open the URL listed in the text messages, however, this can become another gateway in which phishing can occur.

What happens if you open the link anyway? It looks like the following screen:

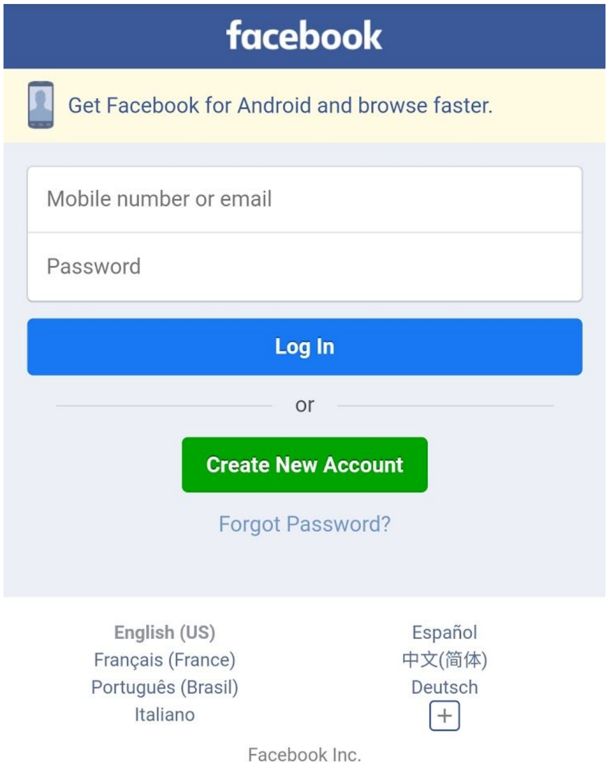


amazon
Welcome
○ Create account. New to Amazon?
● Sign-In. Already a customer?
Email (phone for mobile accounts)
Continue

By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.

Need help?
Conditions of Use
Privacy Notice
Interest-Based Ads

© 1996-2019, Amazon.com, Inc. or its affiliates



Get Facebook for Android and browse faster.

Were you able to spot the difference? Probably not, as the site is a direct copy of the original

For this reason, identifying based on only the appearance is nearly impossible. As a countermeasure, there are generally methods such as checking the URL or certificate of the site, but since most of these websites will be accessed from smartphones, it is highly likely that you will not notice the difference in details.

Once the user unknowingly puts in their credentials for the website, the site administrator can steal it. Subsequent pages may even ask for other information as well, such as credit card numbers, addresses, etc. Sometimes, it could go even further and have the user install an unauthorized app.

So how do we prevent it?

1. Use the Official App to Check Purchase History

An email notification of purchase you do not recall may lead to panic and may cause the mistake of giving away your credentials. So when an email is received that notifies you of fraudulent activity, calm down and check the purchase history through the official app.

If it was indeed, a fraudulent activity taking place, then the user should be able to see it through the app without clicking on the link sent in the email.

2. Try to Avoid Clicking on Links Sent Through Email or Text Message

As in the above, if it was Amazon or Facebook, it is safer to access through the app to confirm the notifications. If you do not have the app, it is also safe to access the site through google.

Even if the message seems safe, it will always be safer to avoid using those links.

In addition to the above, there are detailed countermeasures such as checking the sender of the email, checking the site owner, checking the certificate, and checking the sender if through SMS.

However, considering a smartphone, it is difficult to conduct a detailed survey immediately.

You can eradicate damage from e-mails and SMS simply by making the above two points a habit without thinking about the details.

・What to Do When Phishing Succeeds

It may be different depending on the phishing site, but if you have entered the username and password, immediately change the password.

If possible, change the username as well.

If the same username and password was being used in other sites, make sure to make the changes on those sites as well.

If you cannot log in due to password mismatch, etc., the criminal may have already changed the password.

The damage caused by phishing sites is increasing in both the number of damages and the amount of damage.

Credit card information is mostly stolen during the impersonation of a cashless payment site. If your credit card number or security code is stolen, contact your credit card company and stop your card immediately.

Final Remark

In the future, with the spread of cashless payments, damage to those who do not have knowledge of phishing scams is expected. So the greatest prevention to phishing is to always expect it and to take measures accordingly.

Stay tuned for the next IT News!