MIZUHO

"SECURITY AWARENESS RELATED TO YOUR TRANSACTIONS"

Learn about Targeted Attack Emails !!!

Attackers, using different kinds of <tricks & techniques>, induce you to open an attached file or click a URL access link.

Email Sample targeted Attack Mail

Subject: Invitation to Information Security Seminar for F inancial I nstitutions
From :****@***.com
To: .....@abc.com

Dear Mr / Ms. **

In May 2020, a seminar will be held to report/ discuss results of corporate
survey jointly conducted by ○○ University and Zenginkyo
The briefing session, which is based on the results of the questionnaire, will
be of great help to financial institutions stakeholders in considering the future
direction of information security in financial institutions. Please also see the
reports attached.

We look forward to your active participation.
For details, see the invitation attached.
You can register for the seminar from the address below.
As seminar room capacity is limited, we recommend you to register as soon
as possible.

Register from⇒ https://www.abc.com

Attachments:
Announcements Report

<Tricks & Techniques>

Subject and text are designed to attract targets.

It is necessary to confirm the source address carefully.
In recent years, it sometimes **pretends to be a real company or company email**

It is camouflaged to disguise part of the official website URL so that it cannot be distinguished from the real thing at a glance.

Also, the link destination may be written in meaningful words so you may need to check the actual link destination.

Important!!

For Word/Excel and CSV files etc.
Targeted attack emails using Microsoft Office are on the rise. File extensions can be impersonated.

Attaching a Word file was especially common in FY 2020.

MIZUHO

Email Sample non targeted Attack Mail (random target)

Reminder: [Recent News] [Statement Appointment] Information Updates - New Notice : We sent Summary of your bill has expire, Renews your membership Sunday, Jan 22, 2020 [Statement:- [FWD] Case ID: M68EXXSC

TeamNetflix <noreplyrthismailerid33@ieuwgfiuwegfi
owe.[redacted]
Wed 22/01/2020 02:51

NETFLIX

Automatic payment.

Hi Customer,

Your Auto payment cannot process.
Your subscription period will end on Wed, January 22, 2020.

Click Here to update payment method

please update your payment methode for continue Netflix feature.

The Netflix Team

< Points to notice >

[Subject: From]
As you can see from the email from it's stated as TeamNetflix but the address is noreplyrthismailerid33@ieuwgfiuwegfi.com. Sometimes the email address won't appear until you click on the same. So becareful as the email address looks anonymous and not reliable.

[Text]
The content of the email address pretending to be from NETFLIX, requesting the changes of the payment method as the subscription will end on certain date. Normally when subscription end or payment due, there won't be any request to update payment method but they will inform that they are unable to automatically process the current payment using the previous method and ask us to register new payment method through apps or website.

[Link]
If we are not aware and we click on this link, it will direct you to other page where it requested you to input your details and your payment methods.

How to Protect Yourself from Frauds aimed at **YOUR** companies

1. Protect your computer system from being hacked

- ✉ Your software should be kept updated.
  - ✓ the operation system
  - ✓ the application software
  - ✓ the antivirus software
- ✉ The attached files should be encrypted with complicated passwords when you communicate with outside counterparties by email.

2. Check the received email or call

- ✉ Employees and executive officers who might receive emails or calls requesting to send funds should make sure to check the received emails or calls.
  - ✓ Is the address or the phone number of the sender completely the same as usual?
  - ✓ Is there a sudden request to send the funds to a new bank account?
  - ✓ After noticing a new bank account, is it located in a country or area irrelevant to the business transactions?
  - ✓ Is it an URGENT email which requires an immediate remittance?
  - ✓ Is the sender someone with whom you do not usually get in direct touch?

3. Confirm the request when the emails are suspicious

- ✉ If you receive a suspicious email or call, you should confirm whether it is legitimate.
  - ✓ Contact the person requesting the remittance and confirm the authenticity of the contents of the e-mail or telephone.
  - ✓ If you have to use an email to confirm it, do not REPLY but FORWARD it putting the correct address manually.

4. Build an inner system of procedures to conduct those actions 1 to 3

- ✉ If you receive a suspicious email, you should confirm whether it is legitimate.

MIZUHO

THANK YOU

PT. Bank Mizuho Indonesia