Phishing trends in Japan

Council of Anti-phishing Japan
Shinichi Tankyo
Table of Contents
1. About Council of Anti-Phishing Japan (CAPJ)
2. Phishing Reports
3. Phishing Examples
4. Phishing Trends
5. Awareness Activities (STOP.THINK.CONNECT.)
About Council of Anti-Phishing Japan (CAPJ)
Organization Overview of Council of Anti-Phishing Japan

- Incorporation
  - 2005 Apr.

- Name
  - Council of Anti-Phishing Japan

- Purpose
  - Activity focused on gathering and providing information on phishing fraud cases and technical information to prevent phishing fraud in Japan.

- Member + Observer
  - 102
    - Regular members: 75; research partners: 6; relevant organizations: 14
    - Observer: 7
      - Financial institutions, credit companies, online services, security vendors, etc.

- Chairman
  - Hisamichi OKAMURA

- Steering committee
  - Chairman: Takahiro Kato (Toppan Forms Co., Ltd.)
  - Vice Chairman: Yusuke Karasawa (Japan Digital Design Corporation/SourceNext Corporation)

- Office
  - JPCERT Coordination Center, Inc.
Council of Anti-Phishing Japan’s Activity

Organization for Phishing Countermeasures such as APWG, JPCERT/CC etc.

Credit Card Companies
Internet Providers
Security Providers
National Consumer Affairs Center of Japan

Provide Information

Credit Card Companies
Online Retailers
Security Providers

Provision

Collecting information & raising awareness
Phishing trend analysis
Consideration of technical & legal measures

Council of Anti-Phishing Japan

Observers

Relevant Ministries and Agencies such as Ministry of Economy, Trade and Industry etc.

Provide Information

Enquiry

Emergency Information/Announcements
Revised Guideline (WG activities)
Phishing Report etc.

Posting Information

Exchange Information among members

General Meeting/Information Exchange Meeting
Study Group
Working Group Activities etc.

Exchange Information

Awareness-Raising Activities

■ Phishing Measures Seminar
■ STOP, THINK, CONNECT

Academic Research

■ Early Detection of Phishing Site
■ Full Picture of Phishing Scams
Reception Status of Phishing Reports
Rapid increase since 2018
Tendency to double in 2019 and 2020

Source: Council of Anti-Phishing Japan
Number of Phishing Reports (Monthly, 2020)

- Exceeded 20,000 per month in August 2020

Source: Council of Anti-Phishing Japan
Increase in phishing sites operating in different domains in a short period of time

Source: Council of Anti-Phishing Japan (Data up to August for 2020)
By Brand (Monthly, 2020)

- No significant fluctuation in the number of brands misused
- In September, the top four brands of Amazon, Rakuten, Mitsui Sumitomo Cards, and LINE account for approximately 93.2% of the total number of reports.
Phishing Examples
Fake Ads Guidance

- Fake ads that appear in Google searches

Example of a fake advertisement directed to phishing site

Emergency: phishing BTCBOX (2020/09/28)
Phishing Sites collect a lot of Information

- **Exploited information**
  1. ID/password
  2. Address, Date of Birth, Telephone Number
  3. Credit card information
  4. 3D Secure ID/password
  5. Copy of my number card, driver's license or password
  6. Copy of the credit card
  7. Copy of the residence certificate

---

Emergency information: phishing to make Rakuten (2020/06/25)
Phishing Trends
Recent Delivery of Phishing E-mails

- Mass-delivery phishing e-mails
  The following two types of bulk distribution are noticeable

  - Delivery using spambots
    - Transmit from IP addresses in and out of the country, direct delivery
    - The sender's e-mail address can vary (proprietary domain)
    - Be distributed over and over to a large number of destinations in the same text or URL
    - Recipients of the same domain often list their email addresses

  - Distribution via facilities (servers) of domestic operators
    - The sender's e-mail address may be spoofed, but it uses its own domain and the company's domain.
    - Passing and Sending SMTP Authentication as a Regular User
    - There are cases where a contract is made with a business operator and cases where a exploited account is thought to be used.
    - The originator was from CN, HK, TW in the scope of the search
    - The source IPs were registered in some DNSBL
Destination Phishing URL

- Specify phishing site directly
  - To acquire many domains and build phishing sites at the same time

- Cases involving multiple redirects
  - It is usually about two steps. Many of Apple's phishing sites are multi-tiered.

- Use of shortened URLs
  - Twitter, Linkedin, bitly, GoDaddy, Frama.link, • • • • • •
Multiple Stages of Phishing Sites

- Leading to phishing sites via abbreviated URLs and relay sites

<table>
<thead>
<tr>
<th>No</th>
<th>Description</th>
<th>Example Redirect Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination URL in the mail</td>
<td><a href="http://aqq22.asrkssnsifsada.org/">http://aqq22.asrkssnsifsada.org/</a></td>
</tr>
<tr>
<td>2</td>
<td>Relay site</td>
<td><a href="http://165.22.53.5/bangkol">http://165.22.53.5/bangkol</a></td>
</tr>
<tr>
<td>3</td>
<td>Relay site</td>
<td><a href="https://sebujakeosk.biz/account1.php">https://sebujakeosk.biz/account1.php</a></td>
</tr>
</tbody>
</table>

- Even if the phishing site is closed, the forwarding site remains for a long time, and the new phishing site is linked to the forwarding site
Server certificates are often used on phishing sites and https are often used.

Survey conducted from January to March 31, 2020
Phishing Sites Hosted on HTTPS

153 entries

2019 Jan

2020 Mar

739 cases

For free SSL certificates

Misuse

The usage of Let’s Encrypt is very high
Improved phishing technics


- Understanding of Japan’s current culture and social dynamics
  - Amazon, Rakuten, LINE, are being targetted
  - Usage of Japanese fonts (used to be other Asian fonts)
  - Domestic delivery agent phishing SMS
Awareness Activities
For enhancing cyber security
Awareness campaign

STOP | THINK | CONNECT™
立ち止まる 考える 楽しむ

STC Awareness Working Group of the Council of Anti Phishing Japan
そのサイト安全ですか？

自らが
探し出したサイトは
安全じゃよ…

ほっ本当に安全？？？
立ち止まって考えよう！

STOP | THINK | CONNECT* 楽しむ

詳細はウェブサイトで http://stopthinkconnect.jp/

ネットバンキング不正送金被害が多発しています。
その銀行サイトは本物？それとも偽物？
クリックするの前に確認を！

そのメール本物ですか？

超有名企業からのメールだけ！
絶対に
立ち止まって考えよう！

詳細はフィッシング対策5か条で。

「クレジットカード番号」を盗まれる被害が発生しています。

・嘘のメールを受け取ったら
・被害にあってしまったら
・情報共有しましょう

協力：情報処理推進機構
承認：東京メトロ

JCCA 日本フィッシング対策協会
Council of Anti-Phishing Japan
Thank You for Your Attention.

- Phishing Information
  - Facebook
    https://www.facebook.com/StopThinkConnectJapan/(Link)
  - Twitter
    @antiphishing_jp

- Phishing Reporting Contacts
  - Mail to "mailto:info@antiphishing.jp"!
  - For details, "https://www.antiphishing.jp/contact.html"

For phishing sites in the JP domain
Contact the council!
If you receive an inquiry from JPCERT or the council, please respond.

Thank you!