THE ART OF

PHISHING

AND HOW TO SAVE YOURSELF

OLIVER VALENTINO

- Security Analyst @ Bukalapak
- Previously Security Analyst @ Security consultant

WHAT IS PHISHING

- Wikipedia : **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

- Oxford Reference : A form of fraud, often using forged e-mails or web sites, that tries to persuade users to disclose usernames and passwords for online bank accounts or other valuable resources.

TYPE OF PHISHING

- Deceptive Phishing
- Spear Phishing
- Whaling
- Phone Phishing

THE GATEWAY

THE GATEWAY

- Faked Email
- Chatting
- Malicious Web

FAKED EMAIL

INTERNAL

Target Employee of the company

Targeting CEO or high level management

EXTERNAL

Targeting user. mostly posing as official account from the company.

CHATTING

Mostly target user

MALICIOUS WEB

Targeting user

Also use to deceive employee to gain information

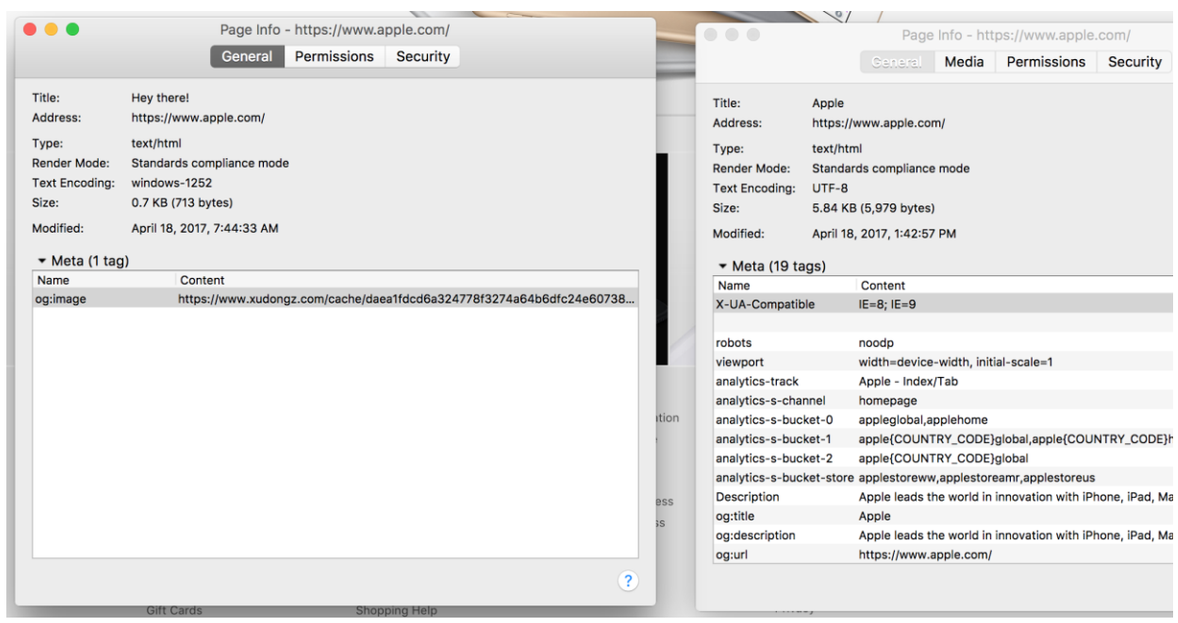
THE TECH

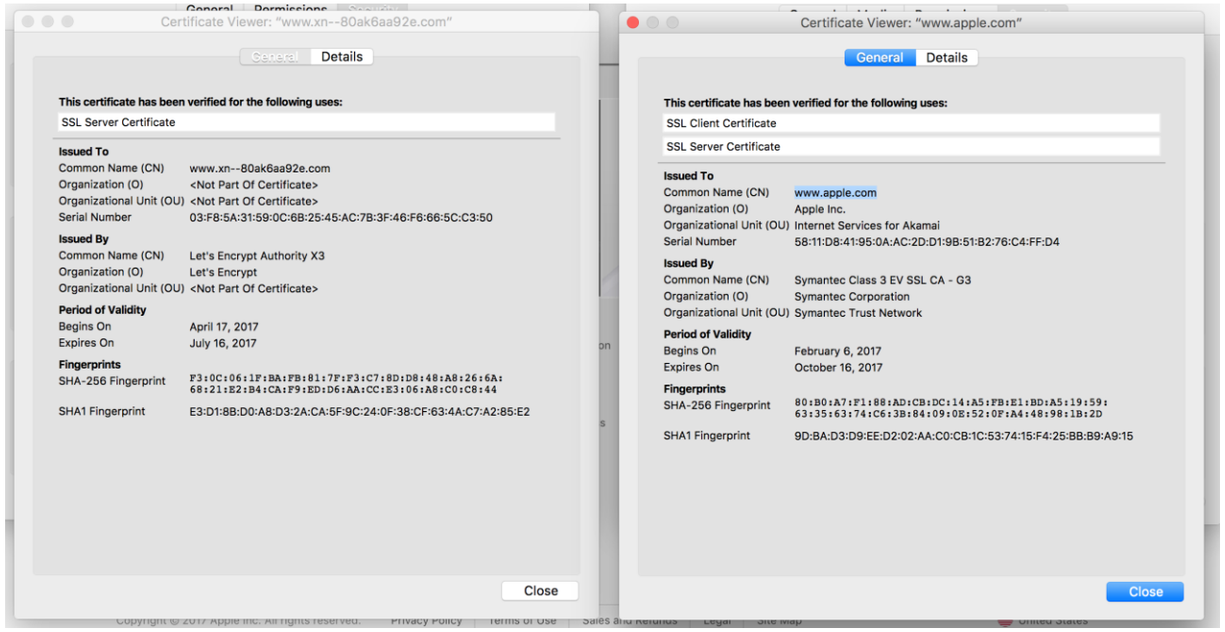
FAKED EMAIL

- Use spoofed email to deceive user, employee, or management
- Use email that looks like the legitimate domain (oliver@bukalapak.com vs oliver@bukalapak.co)
(oliver@singapore.sg vs oliver@sinqapore.sg)
(oliver@bankmandiri.com vs oliver@bank-mandiri.com)

MALICIOUS WEB

- Web designed to look like official website
- Usually they use domain that looks like official website (eg. Homograph attack)
- Most recent technique using punycode phishing attack (https://apple.com/) (https://apple.com/)





SAVE ME!!

FAKED DOMAIN / FAKED EMAIL / MALICIOUS CHAT

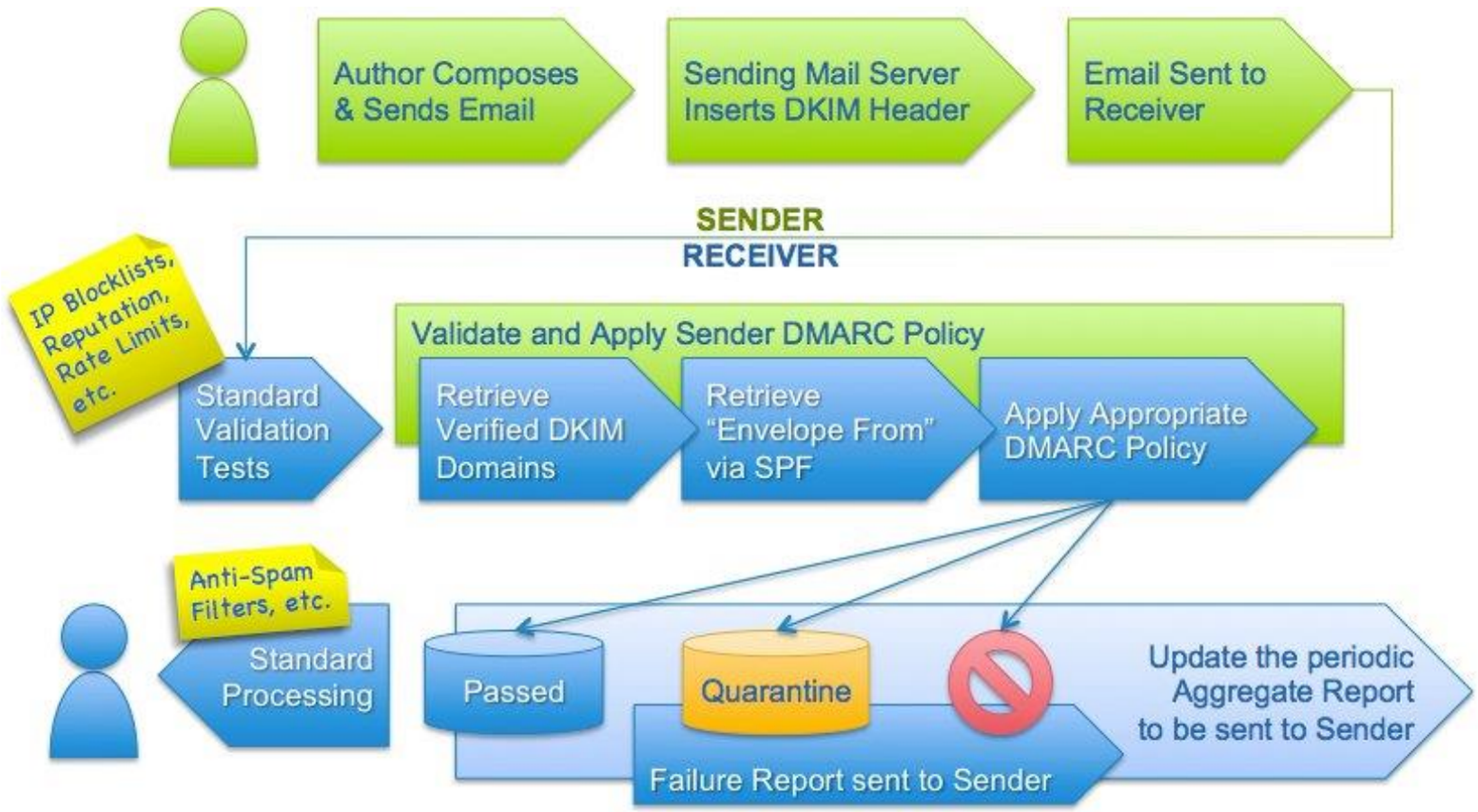
- No technology can defend this kind of attempt.
- Make policy that cover all data or info disclosure process.
- Train and make user and employee aware of the problem, and how to prevent it.

SPOOFED MAIL

- Configure so your official email cannot be spoofed. Usually it involved SPF, DKIM, & DMARC
  - SPF = this checks whether a certain IP is authorized to send mail from a given domain.
  - DKIM = a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is authorized by that domain's administrators.

SPOOFED MAIL (2)

- DMARC = Build up from SPF and DKIM check , adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.



CHAT SYSTEM

- make sure your user know that the user is official form you company or not.
- never allow user to insert link when chat with other user
- NEVER CLICK UNKNOWN LINK FROM UNKNOWN SENDER!!

MALICIOUS WEBSITE

- Create awareness program that contain security awareness.
- NEVER CLICK UNKNOWN LINK FROM UNKNOWN SENDER!!
- Never carelessly input your credential. Make sure you double-check

PUNYCODE

- No known mitigation for chrome or opera.
- Not affecting browser other than Chrome, Firefox, and Opera.
- For Mozilla Firefox
  - get to config page
  - search puny code in search bar
  - find parameter **network.IDN_show_punycode**, select **toggle** to change the value from false to **true**

THANK YOU