



Professional Information Security Association

Build a Secure Cyberspace 2019 – Phishing Attack and Data Protection



Frank Chow

Program Director

Professional Information Security Association

<frank.chow@pisa.org.hk>



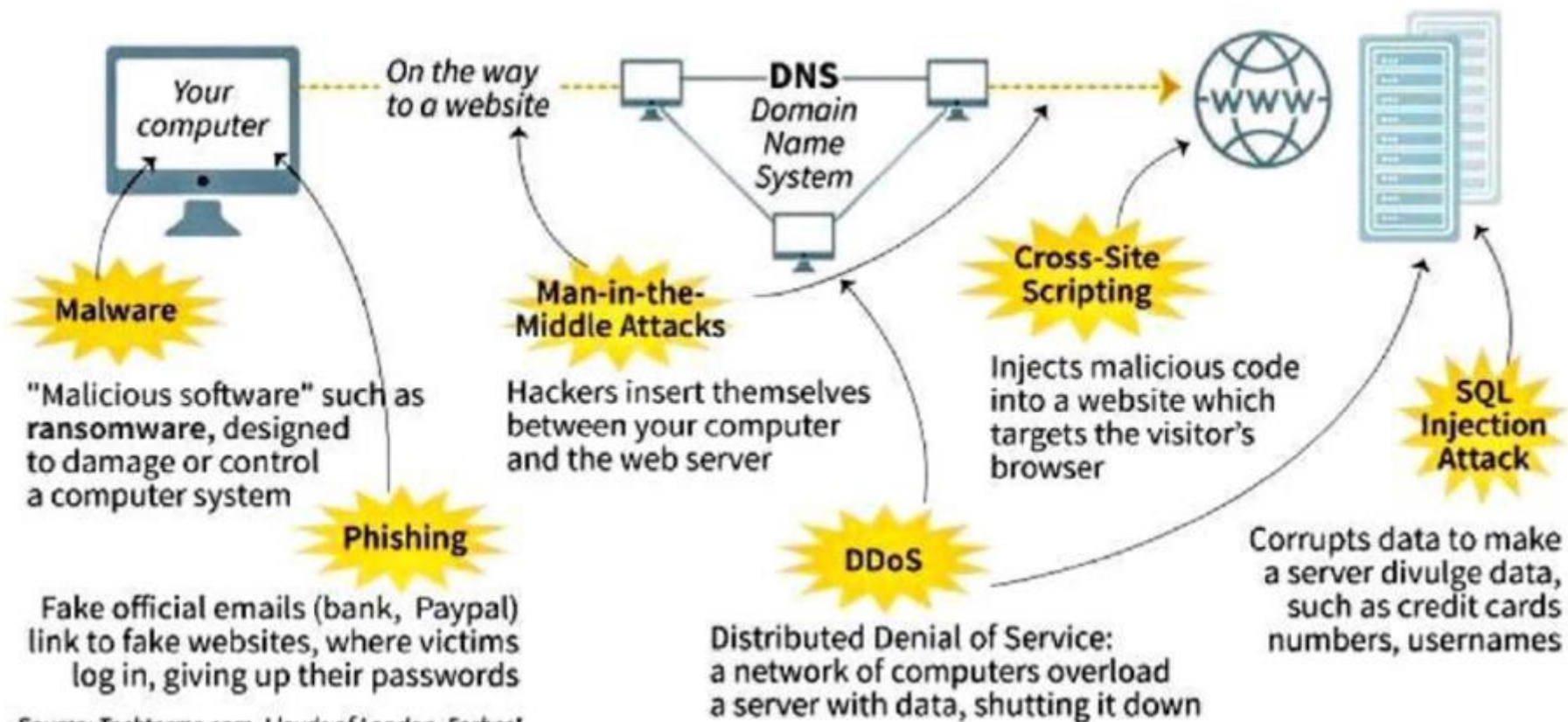
Professional Information Security Association

PISA (專業資訊保安協會)

- Not-for-profit organization
- Facilitate knowledge and information sharing among the PISA members
- Promote the highest quality of technical and ethical standards to the information security profession,
- Promote best-practices in information security control,
- Promote security awareness to the IT industry and general public in Hong Kong,
- Be the de facto representative body of local information security professionals
- <https://www.pisa.org.hk>

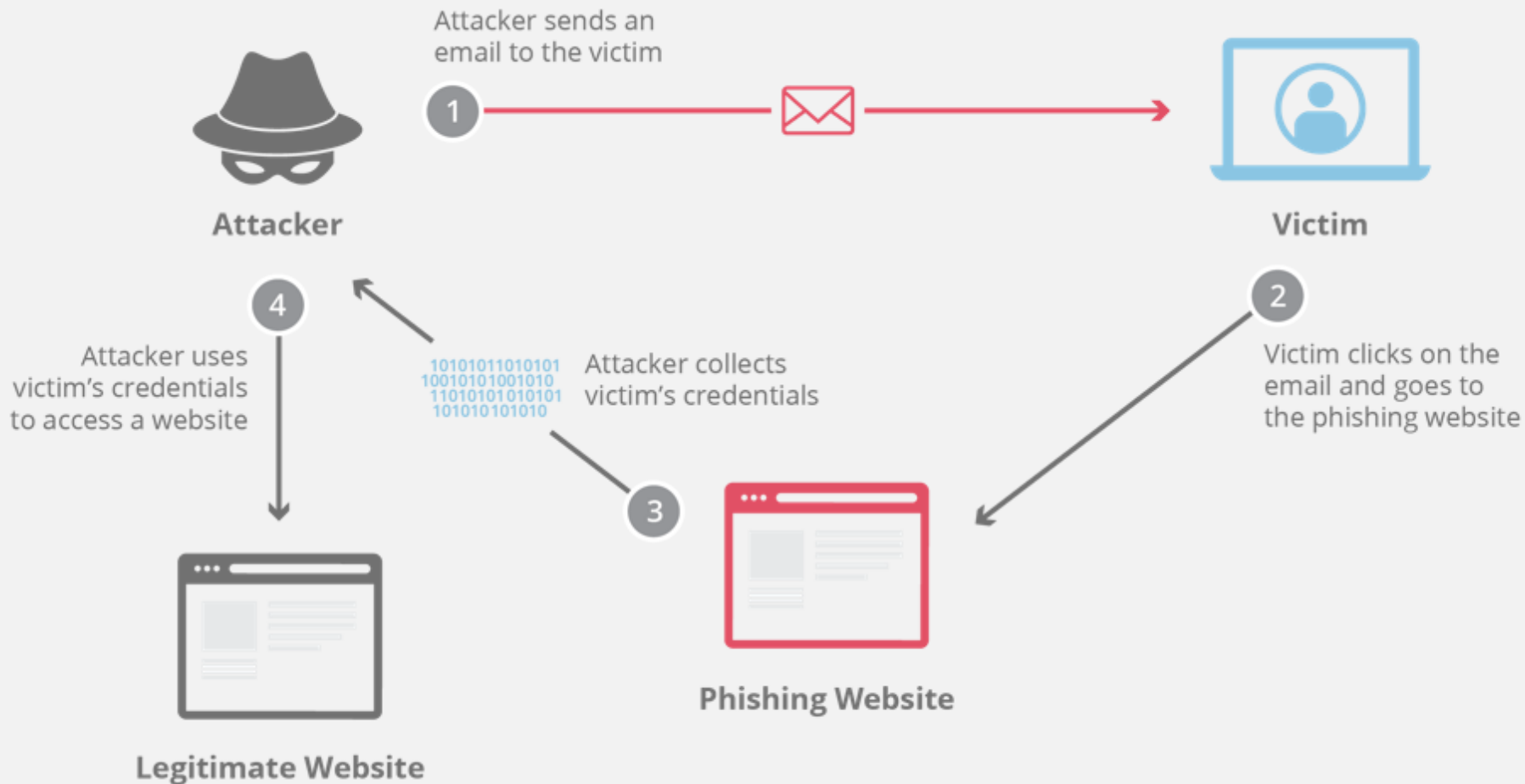


What are the Common Threats?



Source: Techterms.com, Lloyds of London, Forbes*

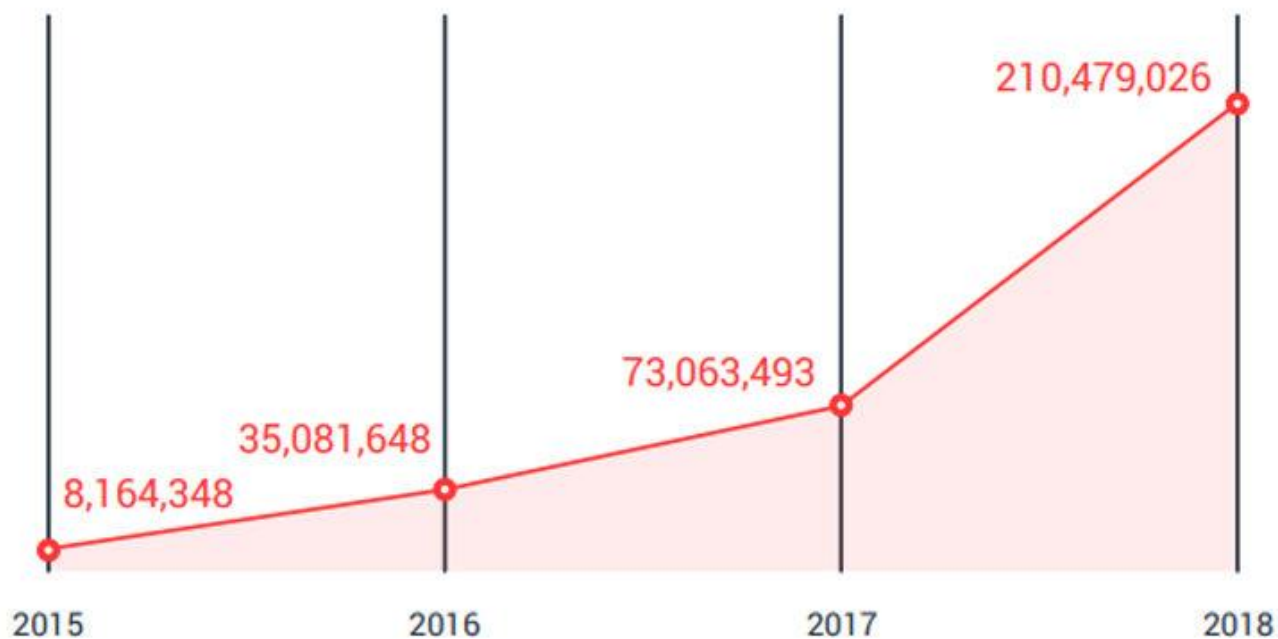
What is a Phishing Attack?





Professional Information Security Association

Phishing Trends

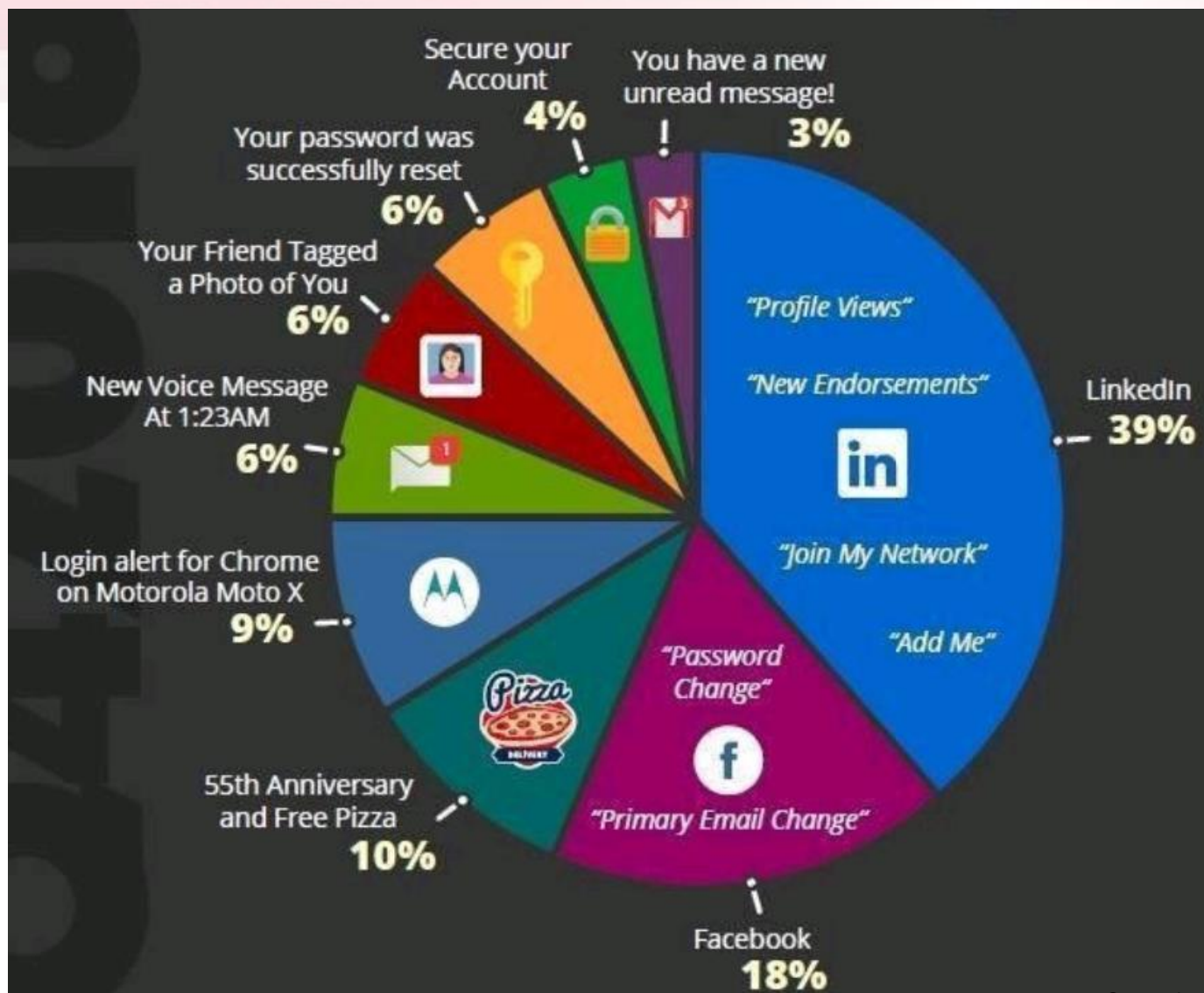


Phishing-related URLs blocked increased over the years, based on data from the Trend Micro Smart Protection Network infrastructure as of Q3 2018.



Professional Information Security Association











Top Social Media Email Subject





Professional Information Security Association

Top 10 General Email Subjects

	Password Check Required Immediately	19%
	Your Order with Amazon.com/Your Amazon Order Receipt	16%
	Announcement: Change in Holiday Schedule	11%
	Happy Holidays! Have a drink on us.	10%
	Problem with the Bank Account	8%
	De-activation of [[email]] in Process	8%
	Wire Department	8%
	Revised Vacation & Sick Time Policy	7%
	Last reminder: please respond immediately	6%
	UPS Label Delivery 1ZBE312TNY00015011	6%



Common "in the wild" Attacks

- Apple: You recently requested a password reset for your Apple ID
- Employee Satisfaction Survey
- Sharepoint: You Have Received 2 New Fax Messages
- Your Support Ticket is Closing
- DocuSign: You've received a Document for Signature
- ZipRecruiter: ZipRecruiter Account Suspended
- IT System Support
- Amazon: Your Order Summary
- Office 365: Suspicious Activity Report
- Squarespace: Account billing failure

Phishing Email Sample (1)

- Too good to be true

The image shows a screenshot of a phishing email. The email header includes the subject 'Award Notification Letter 2008', from 'UKNL@notify.awards.com', date '5/29/2008 9:15 AM', and to 'no To-header on input <unlisted-recipients:>'. The body text reads: 'UK NATIONAL LOTTERY DESK', 'Reference No: ACCU/2007-200', 'Operation Code No: A333/ZZ5', 'We use this medium to notify you of the lottery prize won by your email address. Contact the claims officer below via email:', 'Mr. Graham Wilbert, Tel: +44 704 575 9999, Email: mr.grahamwilbert_uknl@hotmail.com', 'Regards, Notification Department.' At the bottom, the status bar shows the URL 'http://cybertangent.com/UFL.edu'. Four blue callout boxes with white text point to specific elements: 'Foreign Lottery Scams are common' points to the email header; 'You won... but did you play?' points to the body text; 'The email link is really a web link' points to the email address; and 'The status bar reveals the real web address.' points to the status bar.

Foreign Lottery Scams are common

Subject: Award Notification Letter 2008
From: UKNL@notify.awards.com
Date: 5/29/2008 9:15 AM
To: no To-header on input <unlisted-recipients:>

UK NATIONAL LOTTERY DESK
Reference No: ACCU/2007-200
Operation Code No: A333/ZZ5

We use this medium to notify you of the lottery prize won by your email address. Contact the claims officer below via email:

Mr. Graham Wilbert,
Tel: +44 704 575 9999
Email: mr.grahamwilbert_uknl@hotmail.com

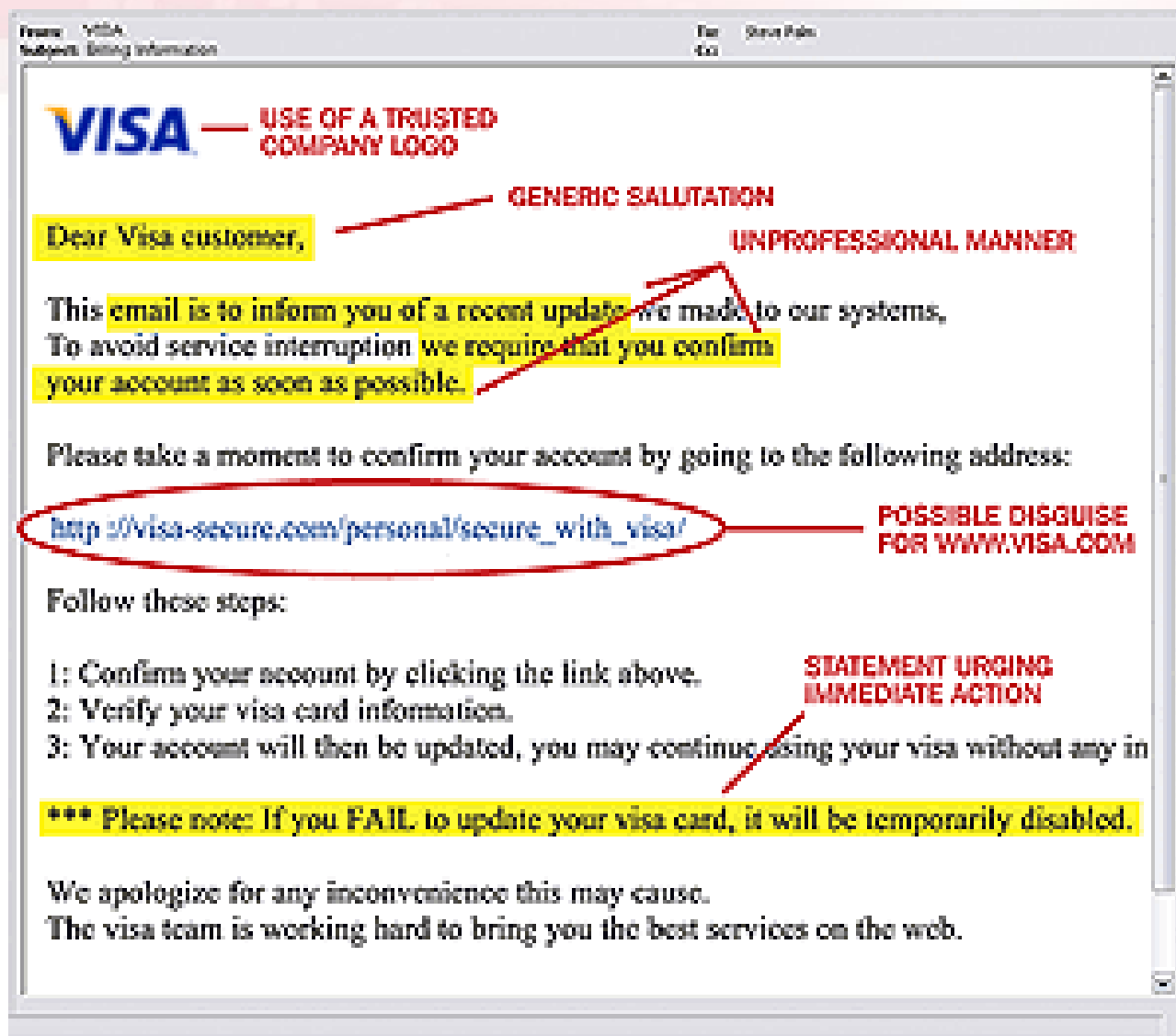
Regards,
Notification Department.

The email link is really a web link

The status bar reveals the real web address.

http://cybertangent.com/UFL.edu

Phishing Email Sample (2)



Phishing Email Sample (3)

From: ouhk.edu.hk [mailto: [REDACTED]@vli.sg] ← Invalid Sender!
Sent: Friday, June 29, 2018 9:29 AM
To: [REDACTED]
Subject: 转发: 最后警告！您的帐户很快被终止（现在更新）

電子郵件截止日期升級

此消息是由可信發件人發送的

這是為了通知您最後一次我們已停止處理您帳戶中的傳入電子郵件

因為您 [https://gofresh.com.pk/koko/163p/cn/bizmail/?email=\[REDACTED\]@ouhk.edu.hk](https://gofresh.com.pk/koko/163p/cn/bizmail/?email=[REDACTED]@ouhk.edu.hk) 服務，並且如果忽略此通知，我們已被迫阻止您的帳戶。
Click to follow link

現在升級

注意：此限制將在我們確認升級成功後暫停。

謝謝，

問候

Customer Care Team © 2018 ← Invalid Team!

This is a fake email sample. DO NOT click on any link in this email.

No contact point available.

With "mouse over" the link, it shows an unknown outbound link.



Phishing Email Sample (4)

User not found

From: Huichang Lin [<mailto:hlin64@uic.edu>]
Sent: Monday, January 29, 2018 2:14 PM
To: [REDACTED]
Subject: Library Services

Contradiction of user email addresses

Non OUHK domain

Dear User,

This message is to inform you that your access to your library account will soon expire. You will have to login to your account to continue to have access to the library services. You can reactivate it by logging in through the following URL. A successful login will activate your account and you will be redirected to your library profile.

http://primo.lib.ouhk.ctuc.ml/primo_library2libweb2action2login.do2loginFn2signin2vid2ouhk2targetURL2myAccountMenu.do23fvid23douhk2lang2en_US/

If you are not able to login, please contact Huichang Lin at hlin2@ouhk.edu.hk for immediate assistance.

Sincerely,

Huichang Lin
OUHK Electronic Library
The Open University of Hong Kong
2768-6983
hlin2@ouhk.edu.hk

This is a fake email sample; DO NOT click on any link in the email



Professional Information Security Association

Watch Out for Emotions

GREED

Phishing emails often dangle a financial reward of some kind if you click a link or enter login information. If an email offers you something that is too good to be true, it probably is.

URGENCY

If an email provides a strict deadline for performing an action - be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.

CURIOSITY

People are naturally curious and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.

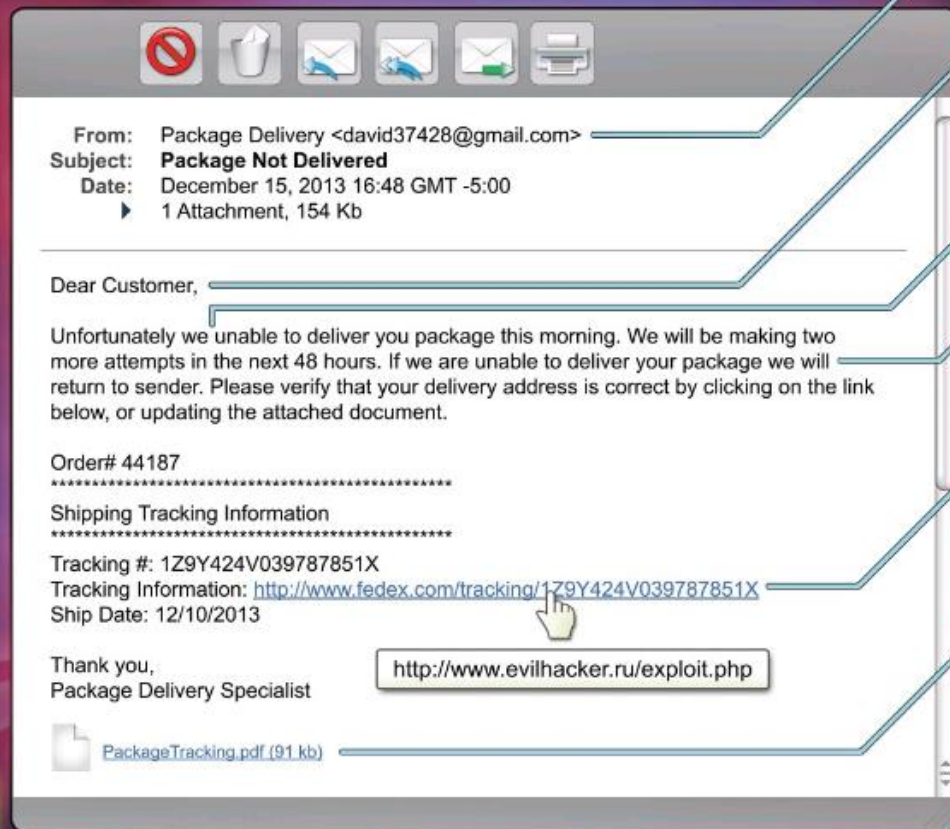
FEAR

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishments should be treated with suspicion.

How to Spot Phishing Email?

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit <http://www.securingthehuman.org/phishing>.



PHISHING INDICATORS

- A** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?
- B** Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?
- C** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.
- D** Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
- E** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.
- F** Be suspicious of attachments. Only click on those you are expecting.
- G** Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.
- H** Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

Phishing Prevention

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.



Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?



Data Protection (1)

STEPS

1

Install a Firewall & Anti-virus Software

The first step in preventing data loss is to install a firewall and anti-virus software. With virus and ransomware attacks coming from spam, phishing, malware, downloaded files, instant messages, web sites, and emails appearing to come from friends, clients and co-workers, you cannot afford to be without up-to-date virus protection.





Data Protection (2)

STEPS

2



Save & Backup Your Files Regularly

The next step is to backup your data with regularly scheduled file and image backups. Be certain that you regularly test your backups to ensure that you can restore your files. Ideally, you'll have a backup located on multiple drives to protect your data from loss due to hard drive failure.



Data Protection (3)

STEPS

3



Keep an Offsite Copy of Your Backup

You also need to protect your data from fire, flood or other natural disaster (and from theft), by having an offsite copy of your backup. While cloud backup is an option, if the disaster disturbs your internet connection, it could prevent you from getting back to business in a timely manner.



Professional Information Security Association

Data Protection (4)

STEPS 4



Update All Security Patches

You also need to pay attention to your systems to ensure that critical updates are applied as soon as they are available. Microsoft releases patches to protect users against discovered vulnerabilities. Hackers use these vulnerabilities to craft an exploit for the purpose of accessing computers and networks that have not installed the security patch.

Last but not least ... Spear Phishing

Anatomy of a spearphishing attack

- 1** Hacker makes a list of key personnel in the organisation having the confidential data he wants.



- 2** He looks up the employees on Facebook and other social media to glean their interests.



- 3** Hacker crafts an e-mail malware with an attachment most likely to pique the interest of the targeted employee.



Hacker crafts an e-mail malware with an attachment most likely to pique the interest of the targeted employee.

- 4** Targeted employee gets the e-mail and clicks on the attachment because it's a subject matter that is of interest.



- 5** The malware is released into his computer and it starts e-mailing copies of all documents and other data on it to the hacker.



- 6** Hacker, who may be in another country, receives the stolen information.

©The Star Graphics

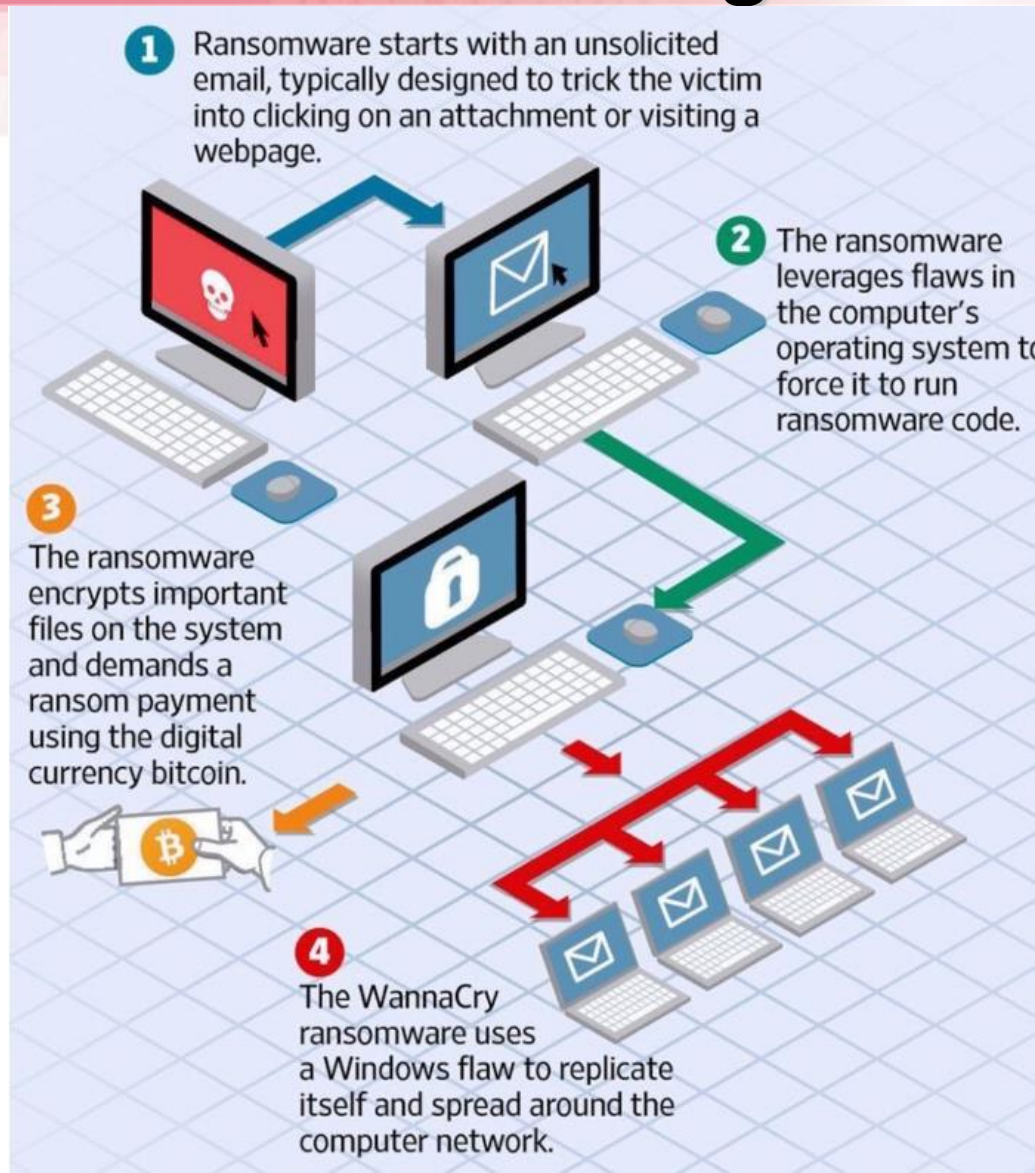


Professional Information Security Association

Last but not least ... Smartphone



Last but not least ... Phishing+Ransomware





Professional Information Security Association

Thank You

<frank.chow@pisa.org.hk>