EFFECTIVE ANTI-PHISHING STRATEGIES & EXERCISES

30th Annual FISSEA Conference I Gaithersburg, MD

19 June 2017

@pauboxhq

PAUBOX

#FISSEA30

Hoala Greevy

Founder CEO, Paubox, Inc. - HIPAA Compliant Email Made Easy.

18 years' experience in email security & encryption.

Phishing & Fishing expert. =)

Agenda

I. What is Phishing Today?

II. Threat Landscape

III. Best Practices

IV. Looking Ahead

I. What is Phishing Today?

Overconfidence Dilemma

Display Name Spoofs

Ransomware stealing thunder

I. What is Phishing Today?

It’s always been about the $$$.

I. What is Phishing Today?

Now it’s about Politics too.

Overconfidence Dilemma

2017 phishing study, University of Texas at San Antonio

Fatal Flaw: Most people believe they are smarter than the criminals perpetrating them.

Source: Science Daily

Display Name Spoofs

91% of phishing attacks

Highly targeted

Impersonates someone familiar to the recipient (usually C-Level)

II. Threat Landscape

Bogus

[redacted] has invited you to view the following document:

Open in Docs

Real

Sean Fujiwara has invited you to **edit** the following document:

LACMA

#FISSEA30

Google Docs Phish

Shut down quickly.

Yet millions affected.

Named the app Google Docs

Source: Wired

Ransomware

2015: 1K daily attacks

2016: 4K daily attacks

2017: ?

#FISSEA30

WannaCry at a Glance

Stolen NSA tools

North Korea GDP

150 countries

At least 230K infected

#FISSEA30

Big Tech Companies Get Hit Too

Facebook & Google Phished

Each paid nearly $100M in fake invoices

Impersonated Quanta Computer

Most funds recovered

Source: The Guardian

Insider Threat

Office 365 Accounts Hacked

Wire transfer request sent from actual HR employee mailboxes

18,000 accounts affected (why so many?)

Source: SC Magazine

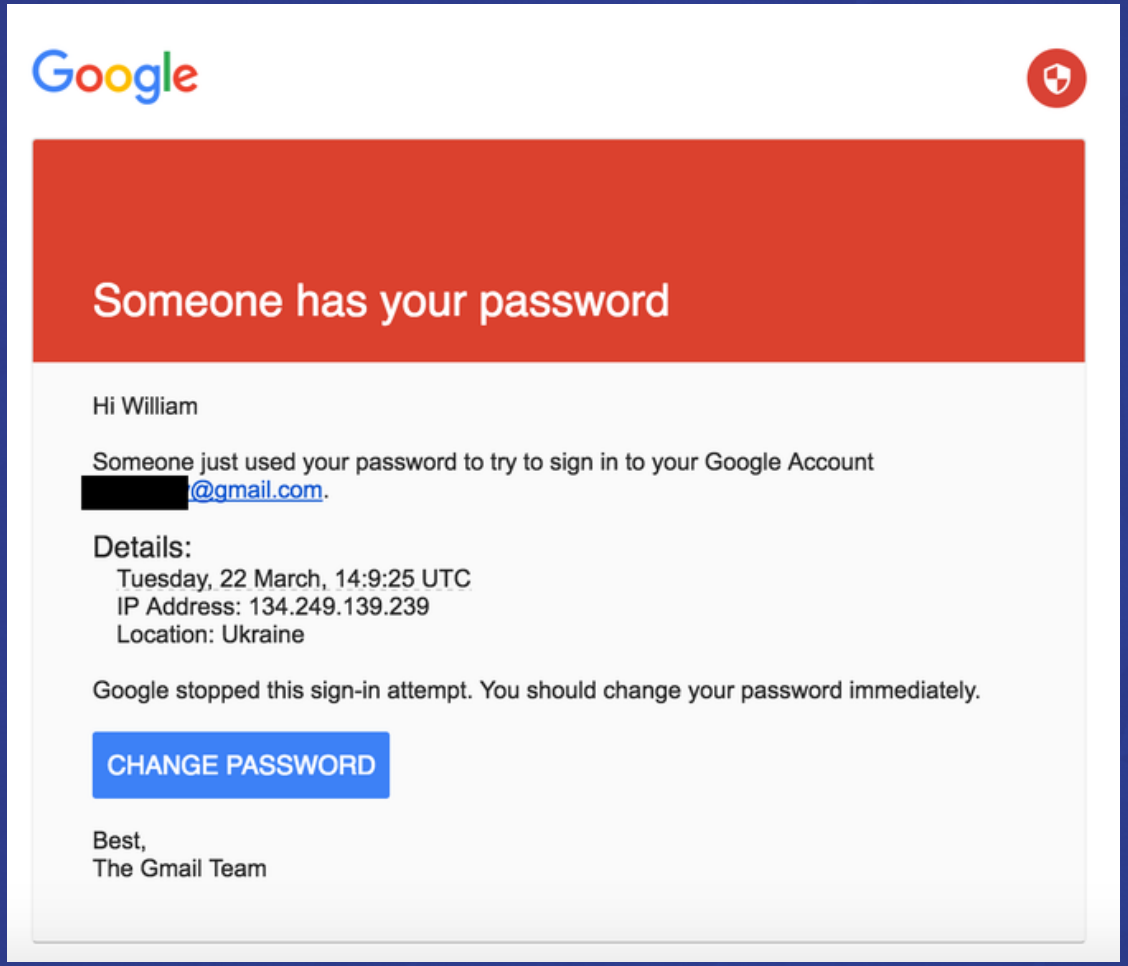
Politics

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

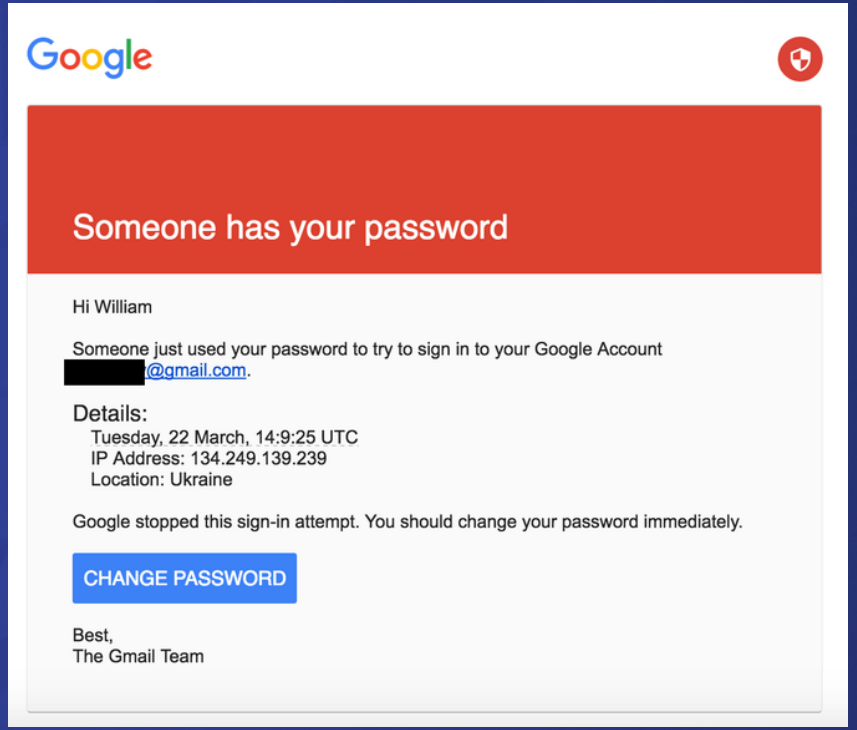

Google
Someone has your password
Hi William
Someone just used your password to try to sign in to your Google Account
[redacted]@gmail.com.
Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine
Google stopped this sign-in attempt. You should change your password immediately.
CHANGE PASSWORD
Best,
The Gmail Team

The Perfect Weapon*

Cheap

Hard to see coming

Hard to trace



* NY Times

Let's Dive In

****
$50 Amazon Christmas Reward
****

Amazon Prime Customer [redacted]

This week and weekend only we have a $50 Christmas Reward for all Amazon and Amazon-Prime members. (Expires 12/24/2015)

Go here to redeem your Amazon Holiday Reward today-- http://shop.radioactivegamingeu.com/inquire

Thanks again for shopping with us.

Amazon, Earth's Biggest Selection

Checkout Bonus No. 5398054
Member ID: UT9662461

Domain Name Shell Game

http://shop.radioactivegamingeu.com

Resolves to:

104.31.65.24
104.31.64.24

Who owns these IPs?

104.31.65.24
104.31.64.24

Cloudflare

Legitimate CDN provider

III. Best Practices

Google Safe Browsing

Macro Policy

Level Up User Training (hold contests)

Nuclear Option: Macs only?

Google Safe Browsing

It’s Free & Constantly Updated

Lots of data sources (over 1B users)

Used in Chrome, Firefox & Safari

Can be used in Email too

Source: Google Safe Browsing

Macro Policy

Re: allowing macros via attachments

Does the business downside now outweigh the upside?

Blog post: We're Clamping Down on Deadly Macros and Ransomware

Arthur Ream

CISO,
Cambridge
Health Alliance

Steak Dinner
phishing bounty

Source: HIMSS Privacy and Security Forum in Boston

Nuclear Option: Macs only?

Something to think about.

IV. Looking Ahead

2FA by default

Clamp down on Domain Registrars

Google Safe Browsing API

IV. Looking Ahead

Machine Learning FTW

Death of the Appliance (Cloud will win)

Port-based Geographic Segmentation

Mahalo!

@hoalagreevy

www.paubox.com

#FISSEA30