MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

LIFE AFTER PHISHING: WHAT'S NEXT

Crane Hassold

Threat Intelligence Manager, PhishLabs

chassold@phishlabs.com

@CraneHassold

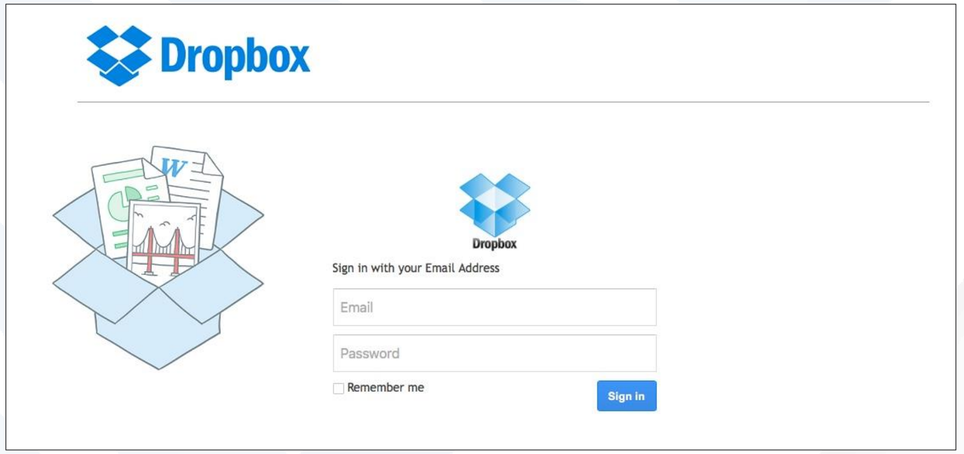
PHISHING: A MODERN TAKE ON A TIMELESS TACTIC

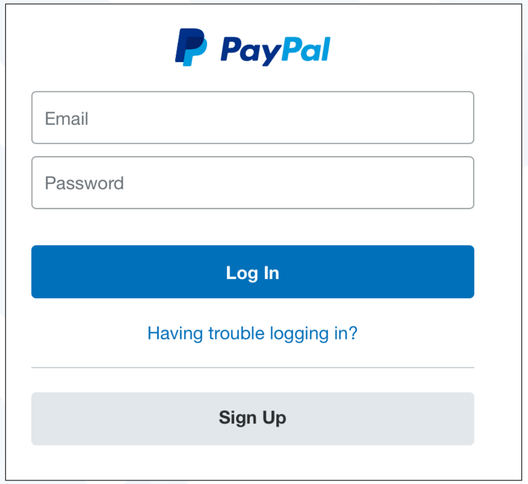
- Phishing = Social Engineering
  - Exploiting human behavior to create a desired outcome
- Social engineering attacks have been around FOREVER
  - Ulysses & the Trojan Horse
  - Victor Lustig
  - Charles Ponzi
  - Frank Abagnale
- Phishing is a merely a social engineering stepping stone
  - Fraudsters will always evolve and adapt to new defenses and new technologies

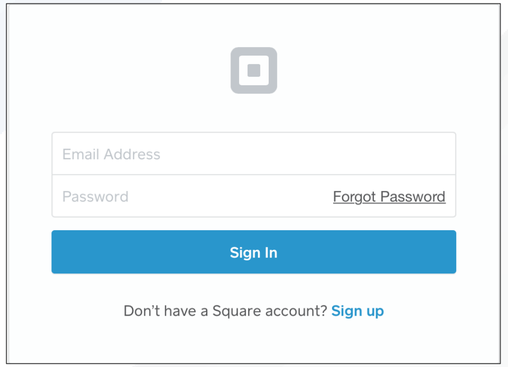
PHISHING TRENDS IN 2017

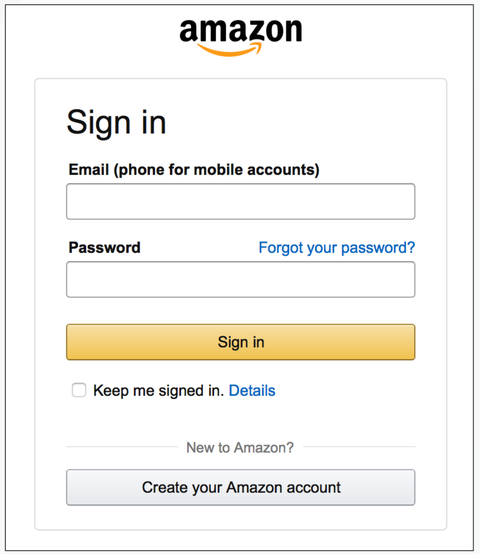
SHIFT IN TARGETING TACTICS

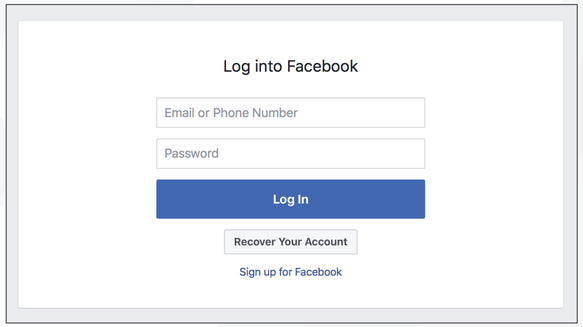
- 2016 saw a shift in **how** victims were targeted
  - Increase in “all-in-one” phishing sites used for mass credential harvesting
  - Driven by the use of email as a primary account credential
  - Facilitates password reuse/reset attacks

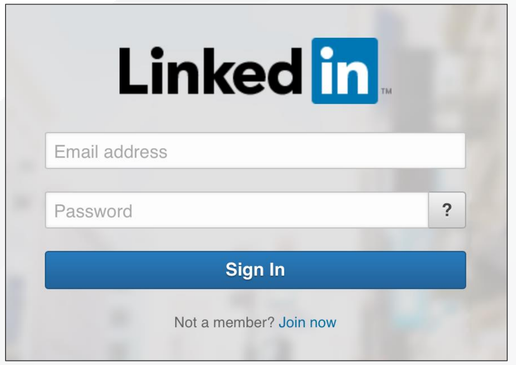






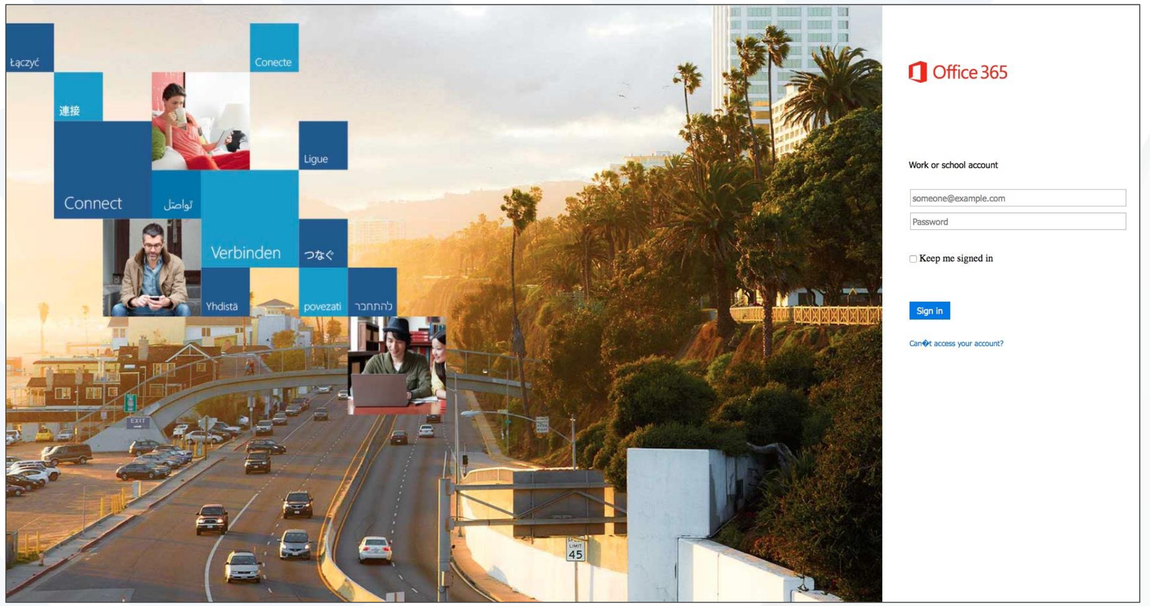


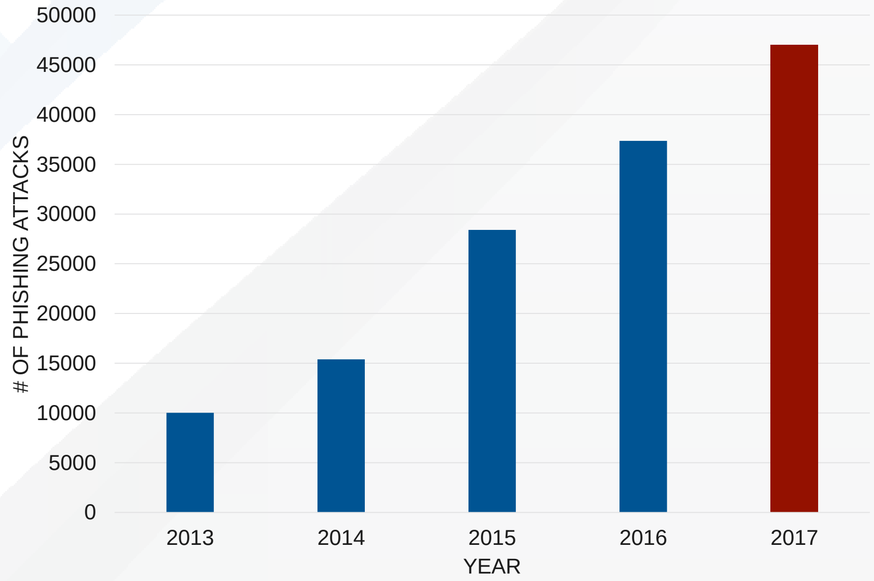




SHIFT IN TARGETING TACTICS

- 2017 saw a shift in **who** phishing attacks target
  - Evolution from individuals to enterprise users
  - Business-oriented services saw major increases
    - Webmail became the #1 targeted industry – driven by Office365/OWA phish
    - SaaS attacks more than tripled – driven by Adobe/ DocuSign phish
  - Follows similar evolution of ransomware targeting in 2016
  - Facilitates BEC attacks, data/IP theft





SHIFT IN TARGETING TACTICS

- 2017 saw a shift in **who** phishing attacks target
  - Evolution from individuals to enterprise users
  - Business-oriented services saw major increases
    - Webmail became the #1 targeted industry – driven by Office365/OWA phish
    - SaaS attacks more than tripled – driven by Adobe/ DocuSign phish
  - Follows similar evolution of ransomware targeting in 2016
  - Facilitates BEC attacks, data/IP theft

From: "Mr Danny" <Customerservice@gmail.com>
Subject: You received an INVOICE via DocuSign
Date: October 16, 2017 at 8:53:12 AM EDT
To: Recipients <Customerservice@gmail.com>

DocuSign

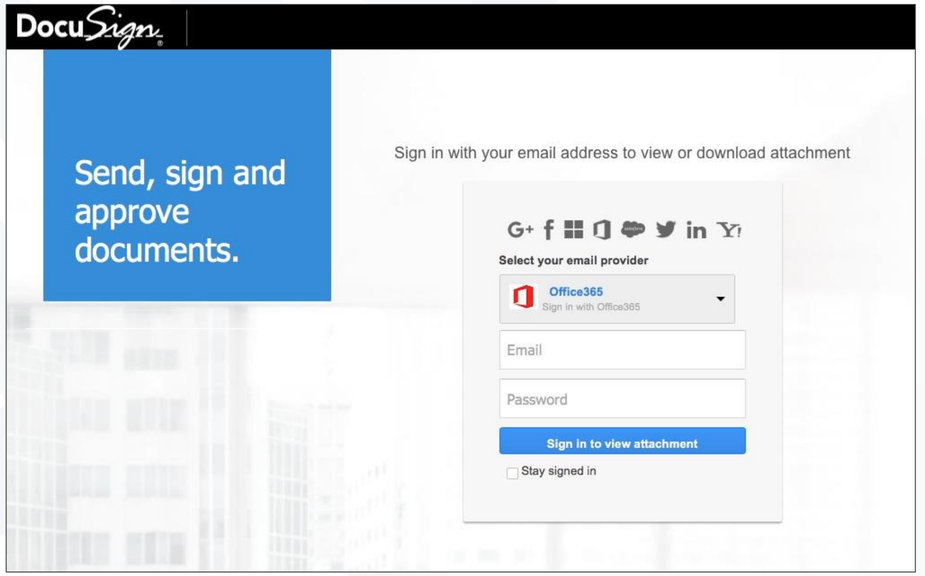
You received an INVOICE via DocuSign

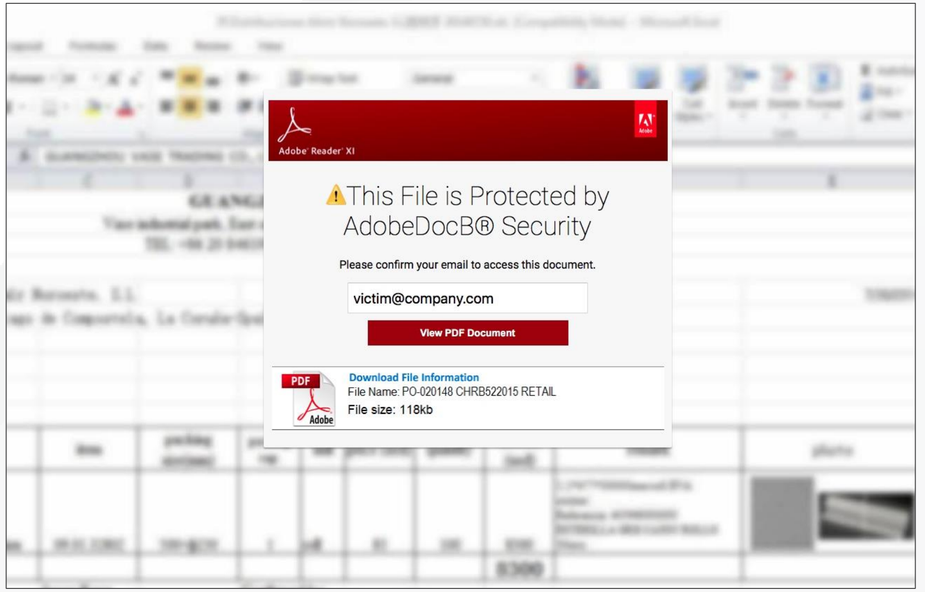
An INVOICE has been sent to you.Your signature is required to access this document. Please apply your electronic signature via DocuSign to access your PDF Document. Click MY ARCHIVE below to access your document.

MY ARCHIVE

Powered By

Google.

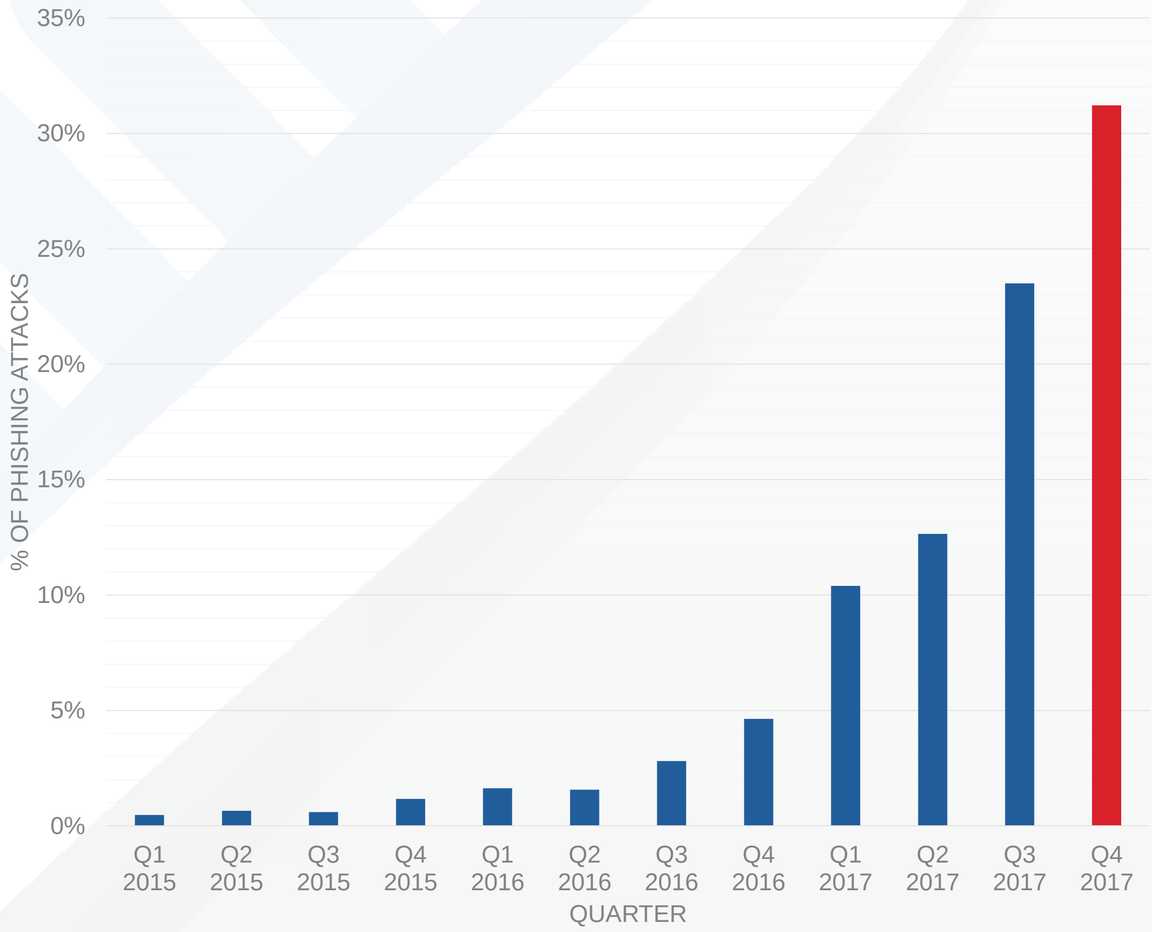




THE RISE OF “SECURE” PHISH

- Phishing sites hosted on HTTPS domains increased significantly in 2017
- In Q4, nearly a third of all phishing attacks were hosted on domains with valid SSL certificates
  - Compared to less than 5% at the end of 2016
- Phishers are using freely available SSL certificates (Let’s Encrypt, Comodo)
- Most HTTPS phish hosted on maliciously-registered domains

WHY?



THE “HTTPS PARADOX”

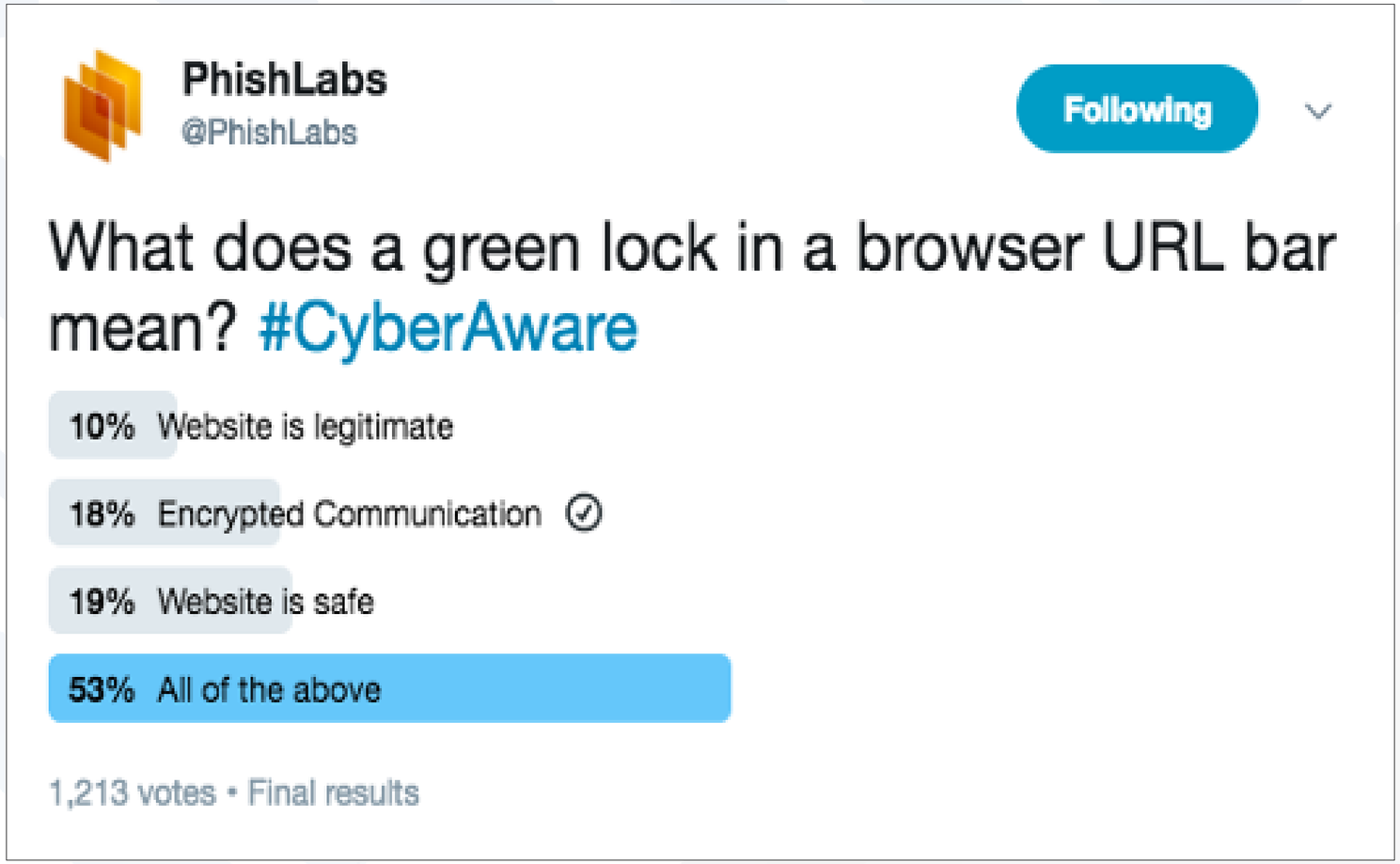
- Users have been conditioned to look for the green lock in the URL bar
- In July, Google will begin displaying a “Not Secure” warning in Chrome for all non-HTTPS websites

- Many people falsely believe this means a website is legitimate or trustworthy

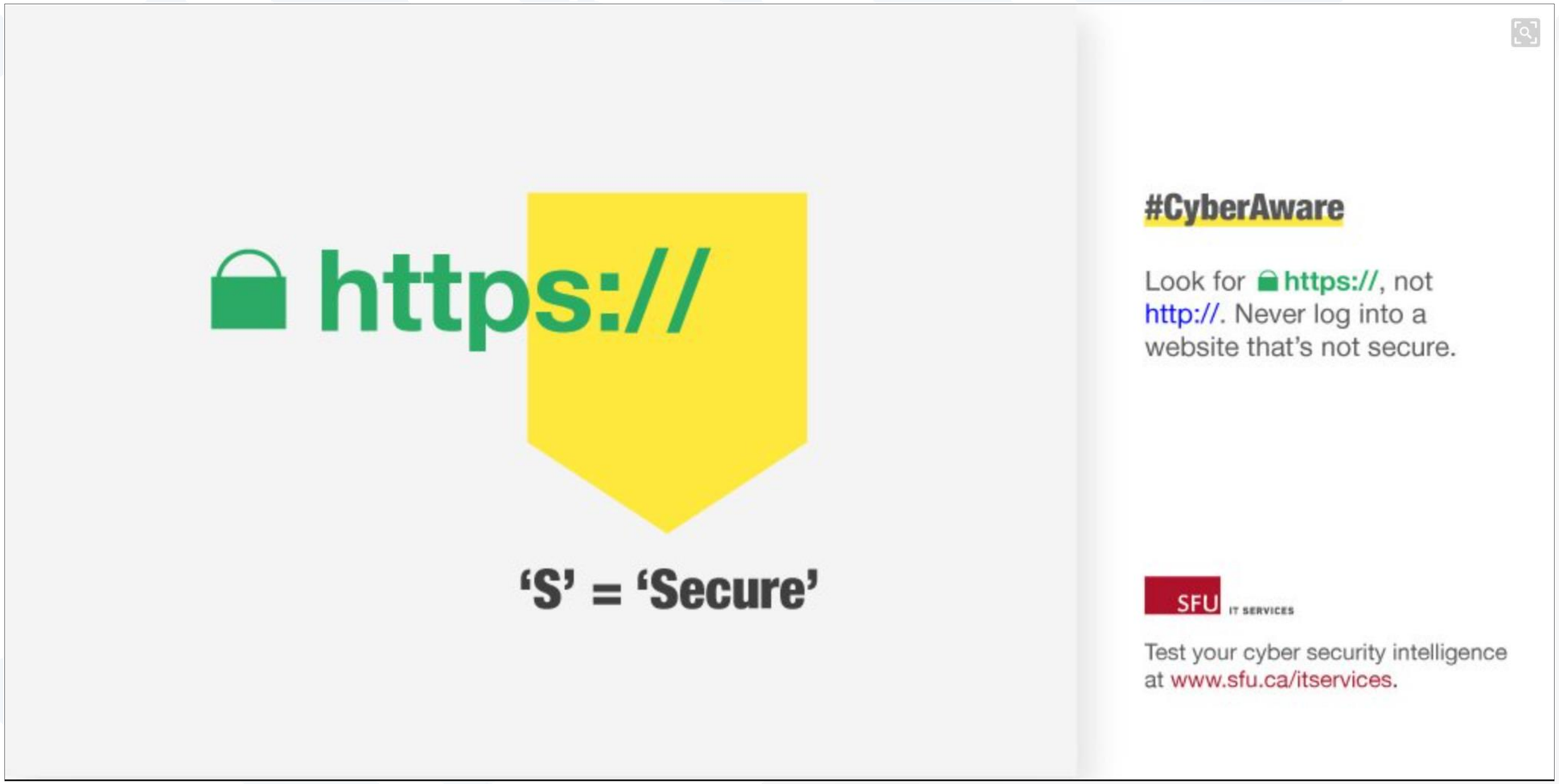
HTTPS = secure transmission of data

HTTPS != authentic website

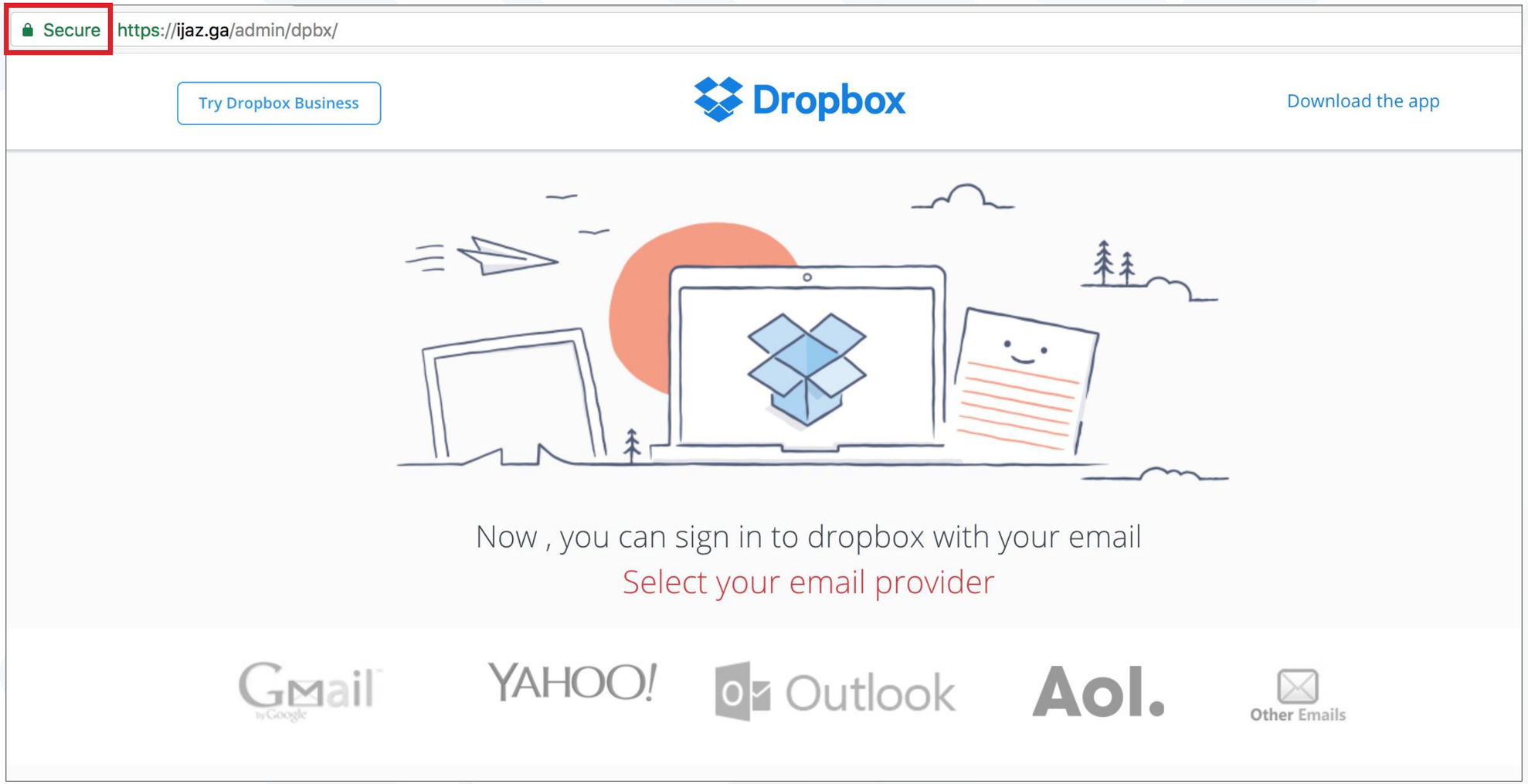
THE “HTTPS PARADOX”



THE “HTTPS PARADOX”



THE “HTTPS PARADOX”



THE “HTTPS PARADOX”

- Users have been conditioned to look for the green lock in the URL bar
- In July, Google will begin displaying a “Not Secure” warning in Chrome for all non-HTTPS websites

- Many people falsely believe this means a website is legitimate or trustworthy

HTTPS = secure transmission of data

HTTPS != authentic website

- Two things will become more common as HTTPS is more commonly used:
  1. Phishers obtaining SSL certificates for maliciously-registered domains
  2. Phishers hosting malicious content on compromised HTTPS websites

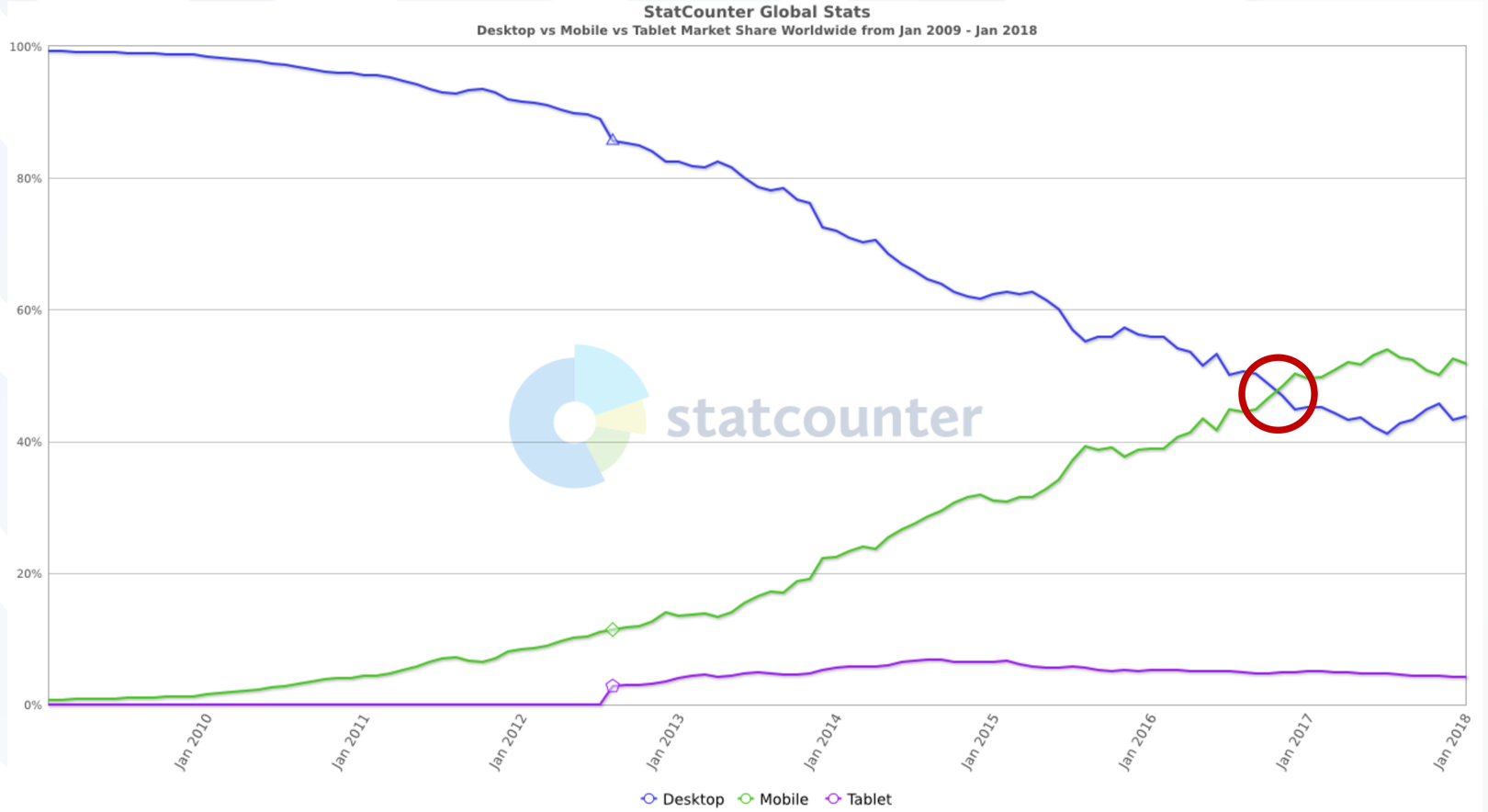
FUTURE ATTACK VECTORS

EMAIL AS AN ATTACK VECTOR

- Email traditionally the primary attack vector for cyber attacks
  - 91% of targeted cyber attacks use phishing as the primary infection vector
- Rise in email attacks in 2016 due to ransomware surge
- Email-based attacks may start to fade
  - User awareness training has been adopted by a growing number of companies
  - Technical defenses are improving
- Threats won’t go away; tactics will simply evolve

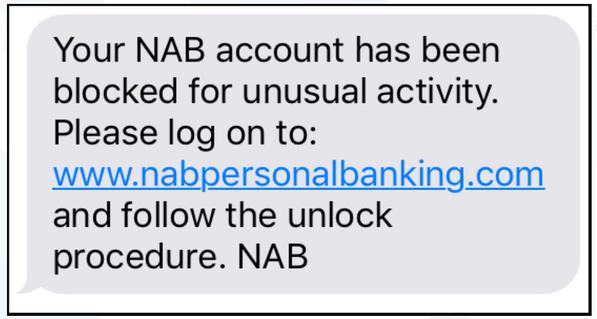
SMS AS AN ATTACK VECTOR

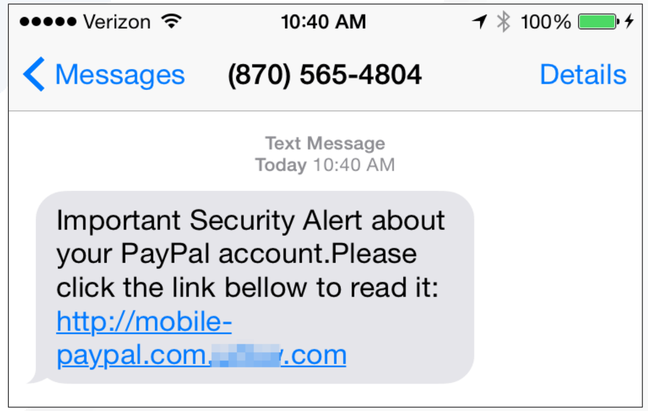
- Mobile devices are becoming the primary way people access the internet

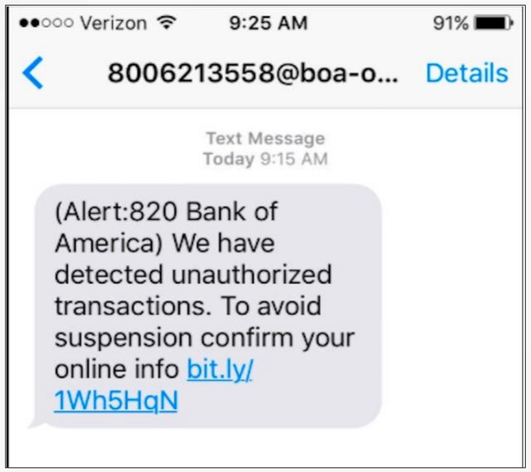


SMS AS AN ATTACK VECTOR

- Mobile devices are becoming the primary way people access the internet
- Security measures on phones have not caught up to email
  - People aren’t conditioned to review contents of SMS

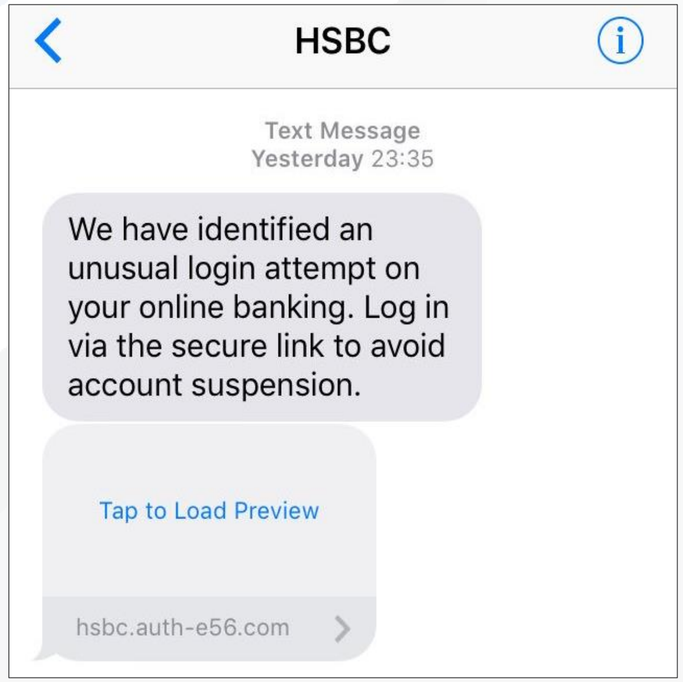






SMS AS AN ATTACK VECTOR

- Mobile devices are becoming the primary way people access the internet
- Security measures on phones have not caught up to email
  - People aren't conditioned to review contents of SMS
  - Previews may give false sense of authenticity
  - Mobile browsers do not block as well as desktop browsers
- Banking Trojans moving to SMS as an infection vector
  - Marcher, BankBot, RedAlert2



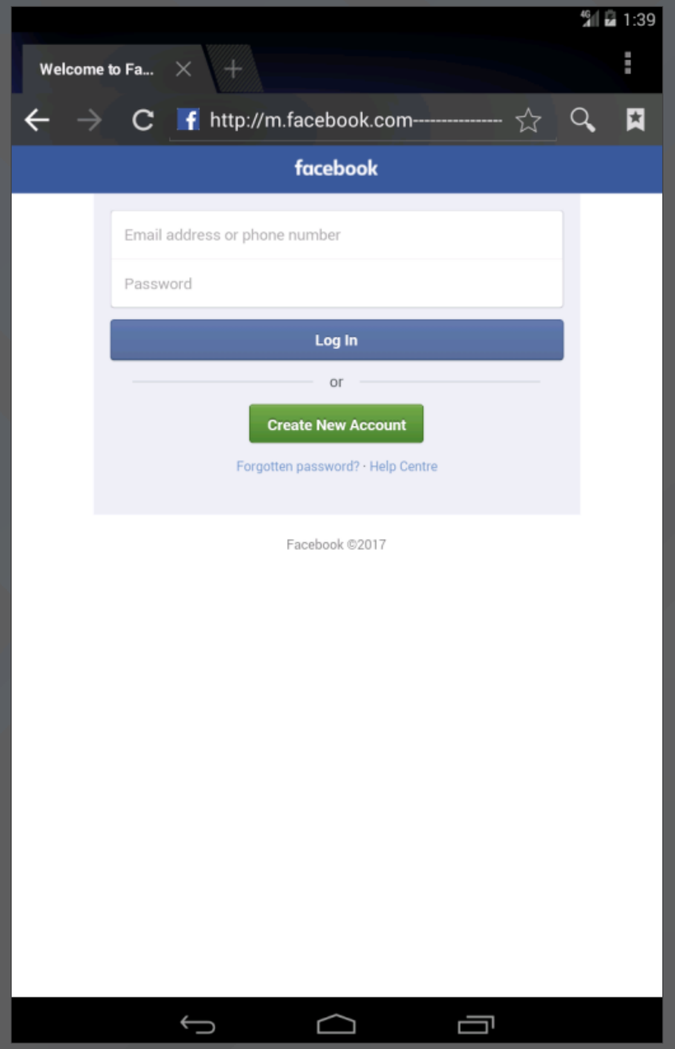
NEW PHISHING TECHNIQUE: URL PADDING

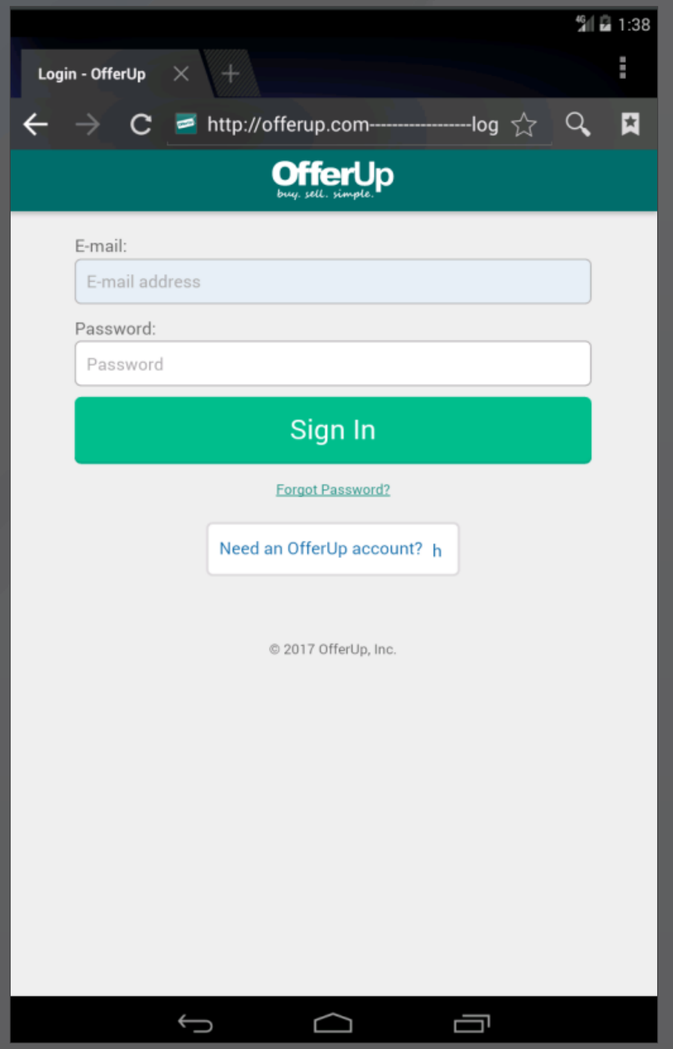
- First observed in January 2017
- Focused on mobile device users
- Subdomain contains legitimate target website followed by numerous hyphens
- Used to obscure real destination

http://m.facebook.com----------validate----step1.rickytaylk.com/sign_in.html

NEW PHISHING TECHNIQUE: URL PADDING

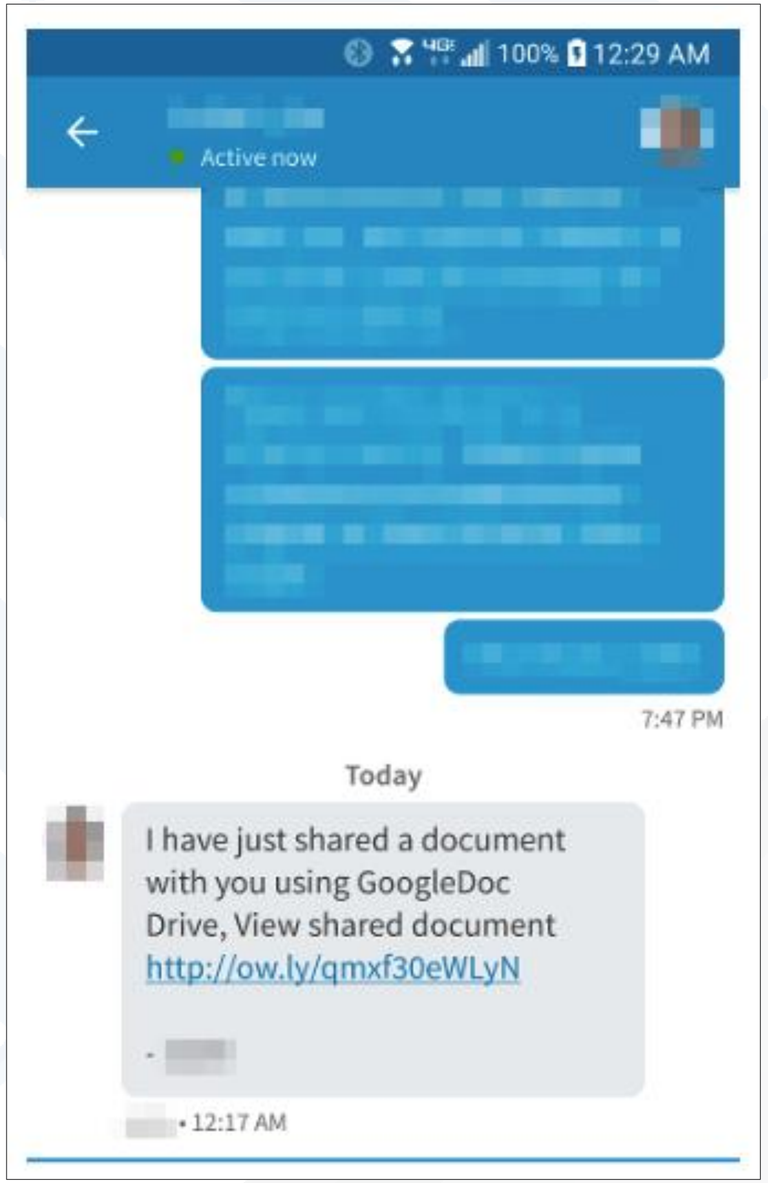
- First observed in January 2017
- Focused on mobile device users
- Subdomain contains legitimate target website followed by numerous hyphens
- Used to obscure real destination
- Brands targeted:
  - Facebook
  - Craigslist
  - OfferUp
  - CenturyLink
  - Visa
  - Apple
  - PayPal
  - Comcast

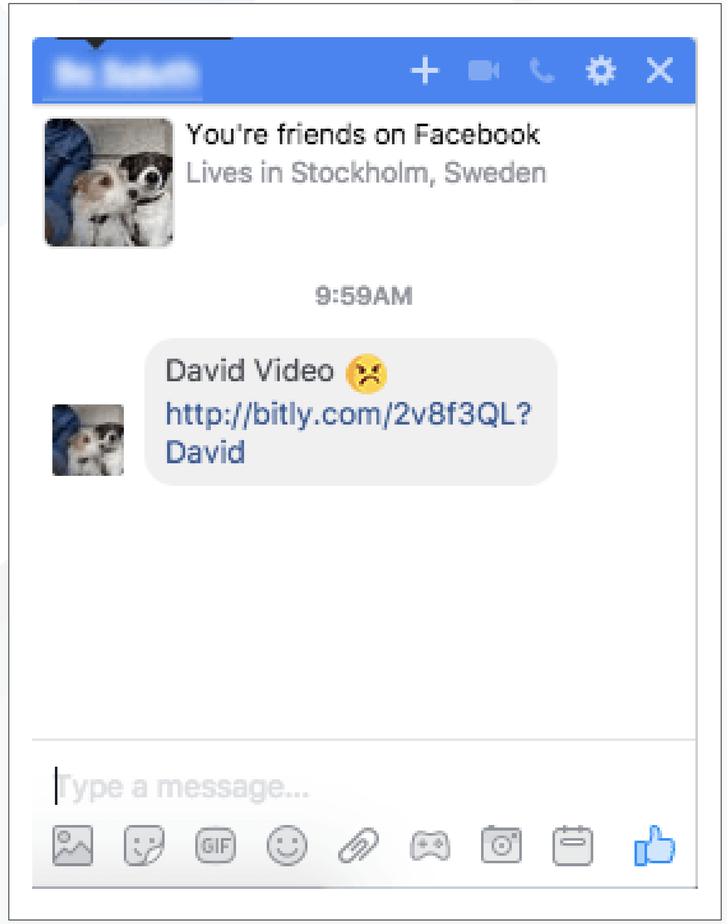




SOCIAL MEDIA AS AN ATTACK VECTOR

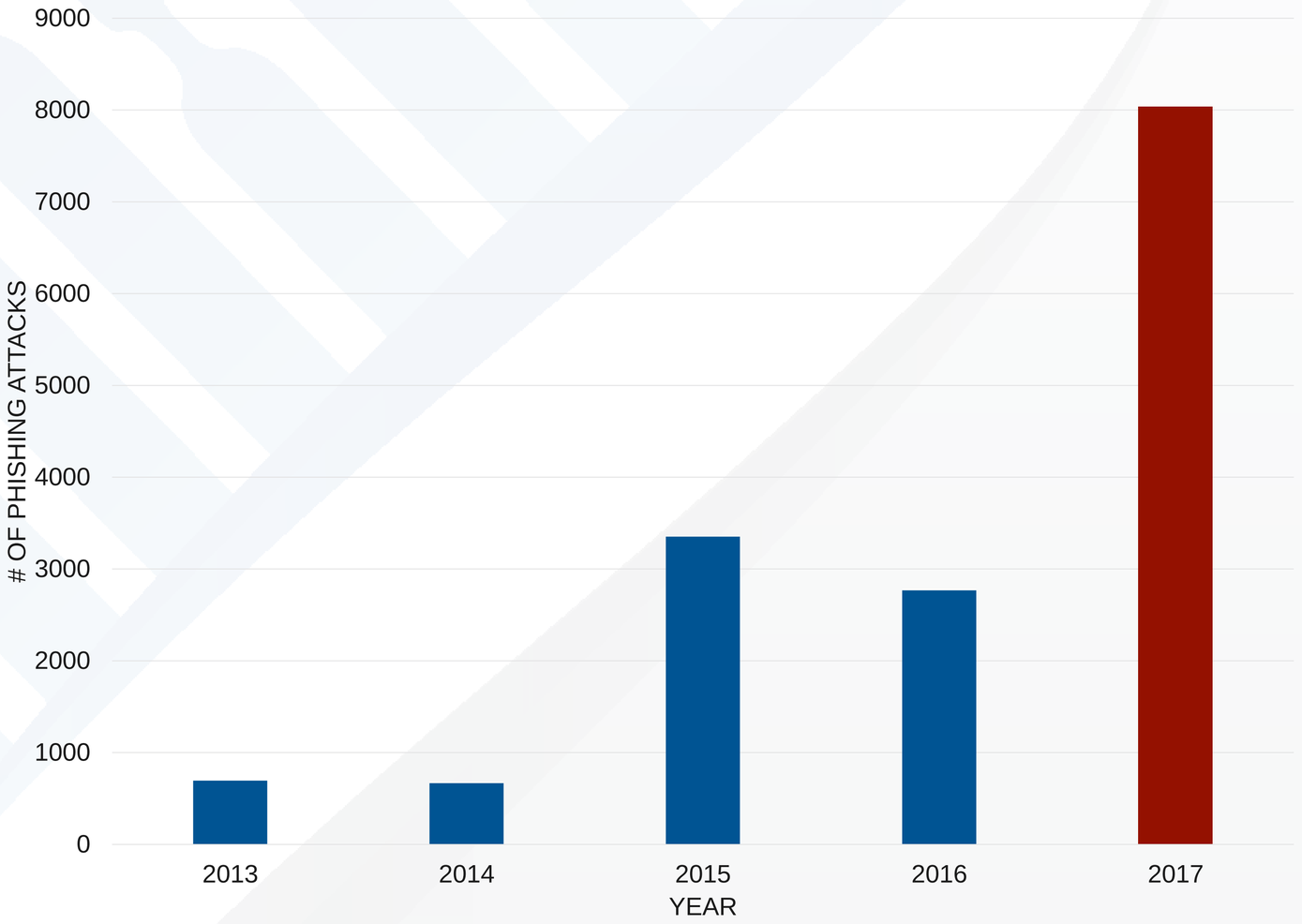
- Gaining momentum as an attack vector due to built-in trust
  - Facebook
  - LinkedIn
- Different from email where there is an inherent *distrust* of unknown senders
- Particularly useful in sophisticated “long con” attacks
- Potential targeting of enterprise accounts outside of corporate networks





SOCIAL MEDIA AS AN ATTACK VECTOR

- Number of social media phishing attacks nearly tripled in 2017
  - Q2 2017 exceeded the attack volume of all of 2016!
- Signals a potential evolution in the use of compromised SM accounts and attack vectors



WRAPPING UP

- Social engineering attacks may evolve, but will never stop
- Targets of phishing attacks shifting from individuals to enterprise users
- HTTPS phish are a serious threat due to poor messaging
- SMS/social media are quickly becoming preferred vectors of attack for phishers

- **We need to constantly think ahead to begin protecting against future threats**

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Crane Hassold

Threat Intelligence Manager, PhishLabs

chassold@phishlabs.com

@CraneHassold