CISC 3325 - Information Security

The Web—User Side

Adapted from *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc.

Phishing Attacks

https://realbusiness.co.uk/tech-and-innovation/2017/08/22/phishing-attacks-soaring-can-minimise-risk/

https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-succ
Search
Sumo
THEATRE
Radio Guide
Story
crime
DETECTIVE

TECHNOLOGY

Phishing Is the Internet's Most Successful Con

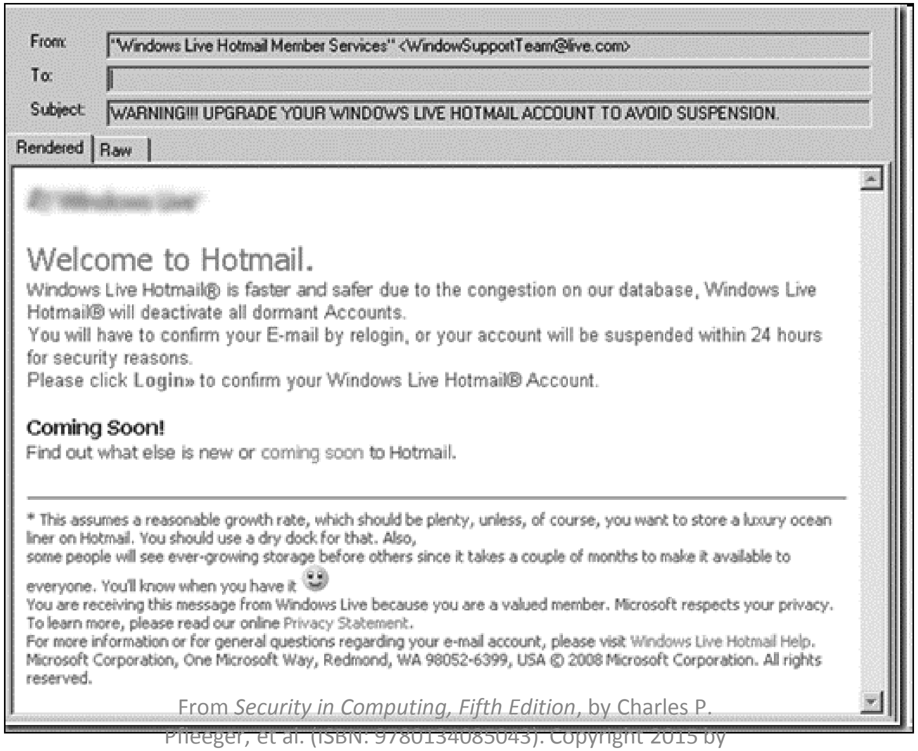
Tricking people out of sensitive information online is far too easy.

QUINN NORTON SEP 12, 2018

https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-successful-con/569920/

Phishing

- A message that tries to trick a victim into providing private information or taking some other unsafe action
- Spear phishing: A targeted attack that is personalized to a particular recipient or set of recipients



From: "Windows Live Hotmail Member Services" <WindowSupportTeam@live.com>

To:

Subject: WARNING!!! UPGRADE YOUR WINDOWS LIVE HOTMAIL ACCOUNT TO AVOID SUSPENSION.

Welcome to Hotmail.

Windows Live Hotmail® is faster and safer due to the congestion on our database, Windows Live Hotmail® will deactivate all dormant Accounts.
You will have to confirm your E-mail by relogin, or your account will be suspended within 24 hours for security reasons.
Please click **Login»** to confirm your Windows Live Hotmail® Account.

Coming Soon!
Find out what else is new or coming soon to Hotmail.

* This assumes a reasonable growth rate, which should be plenty, unless, of course, you want to store a luxury ocean liner on Hotmail. You should use a dry dock for that. Also,
some people will see ever-growing storage before others since it takes a couple of months to make it available to everyone. You'll know when you have it ☺
You are receiving this message from Windows Live because you are a valued member. Microsoft respects your privacy. To learn more, please read our online Privacy Statement.
For more information or for general questions regarding your e-mail account, please visit Windows Live Hotmail Help.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA © 2008 Microsoft Corporation. All rights reserved.

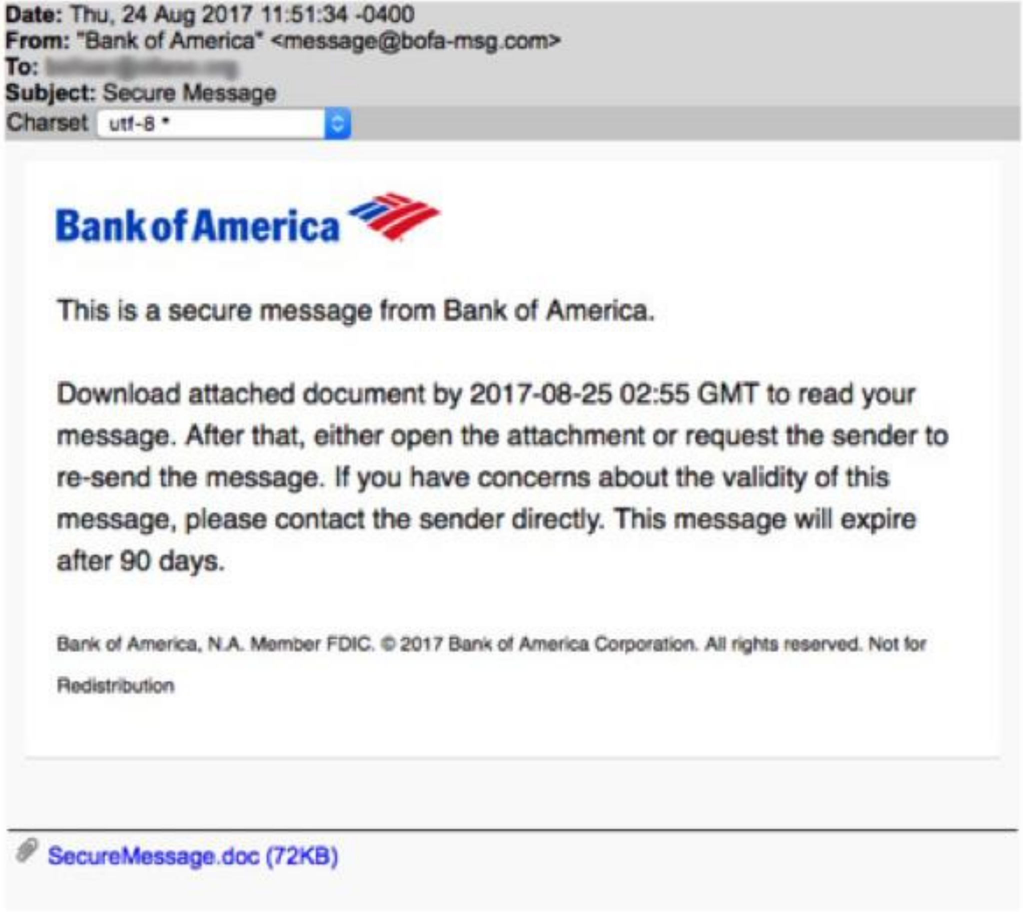
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Phishing Attack

- Fake website created by malicious entities
  - appears similar to a real one
- User is tricked into visiting website
  - Through malicious emails, links
- User inserts credentials and sensitive data
  - Get sent to the attacker
  - Web page then either shows maintenance issues or directs user to real website

http://www.lawpracticetipsblog.com/2017/01/gmail-phishing-attack.html

Example: phishing email



Date: Thu, 24 Aug 2017 11:51:34 -0400
From: "Bank of America" <message@bofa-msg.com>
To: [redacted]
Subject: Secure Message
Charset utf-8

Bank of America

This is a secure message from Bank of America.

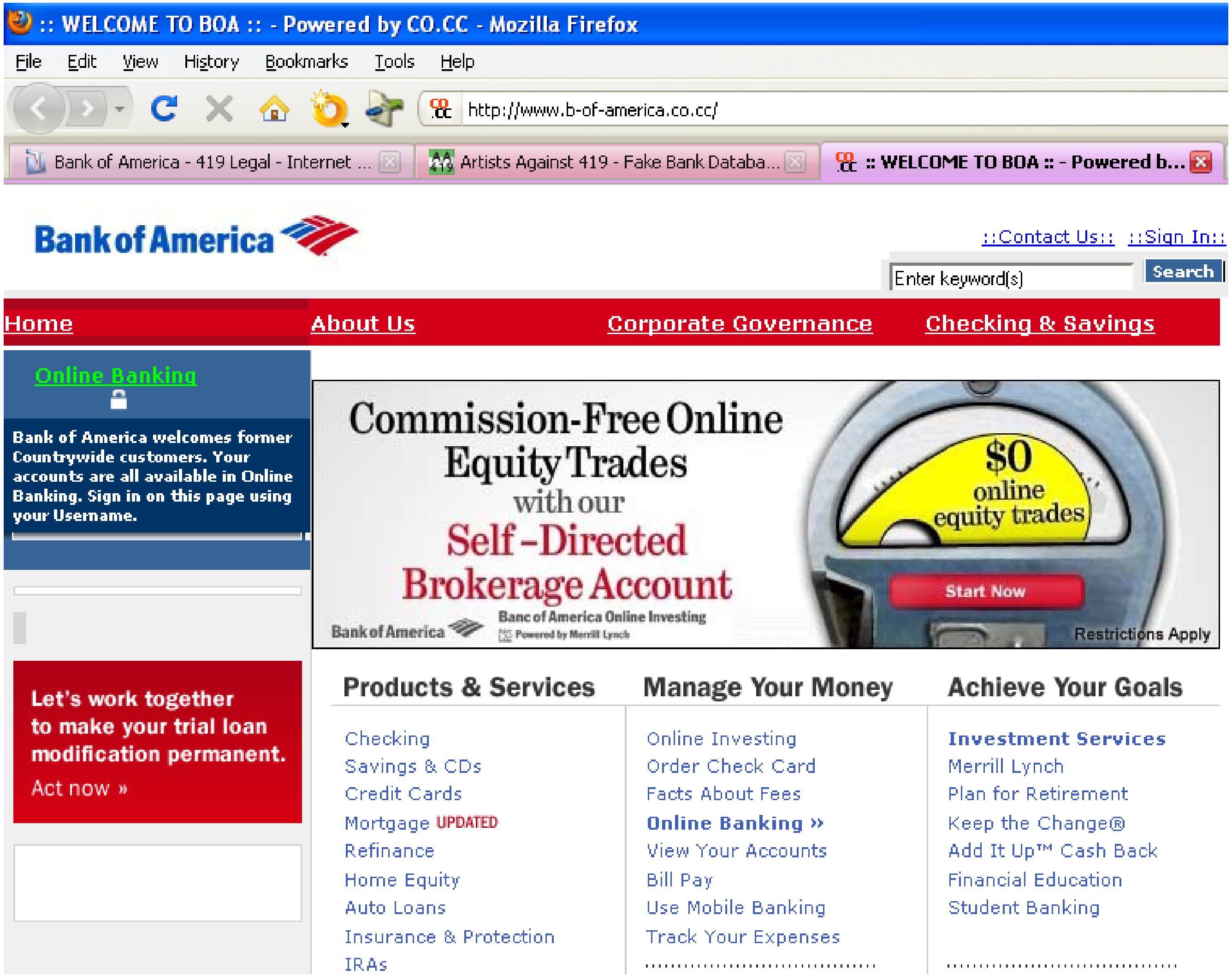
Download attached document by 2017-08-25 02:55 GMT to read your message. After that, either open the attachment or request the sender to re-send the message. If you have concerns about the validity of this message, please contact the sender directly. This message will expire after 90 days.

Bank of America, N.A. Member FDIC. © 2017 Bank of America Corporation. All rights reserved. Not for Redistribution

SecureMessage.doc (72KB)

https://blog.barracuda.com/2017/09/28/threat-spotlight-email-malware-impersonates-secure-bank-messages/

Example: fake bank website


:: WELCOME TO BOA :: - Powered by CO.CC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.b-of-america.co.cc/
Bank of America - 419 Legal - Internet ...
Artists Against 419 - Fake Bank Databa...
:: WELCOME TO BOA :: - Powered b...
Bank of America
::Contact Us:: ::Sign In::
Enter keyword(s)
Search
Home
About Us
Corporate Governance
Checking & Savings
Online Banking
Commission-Free Online Equity Trades with our Self-Directed Brokerage Account
Bank of America
Banc of America Online Investing
Powered by Merrill Lynch
$0 online equity trades
Start Now
Restrictions Apply

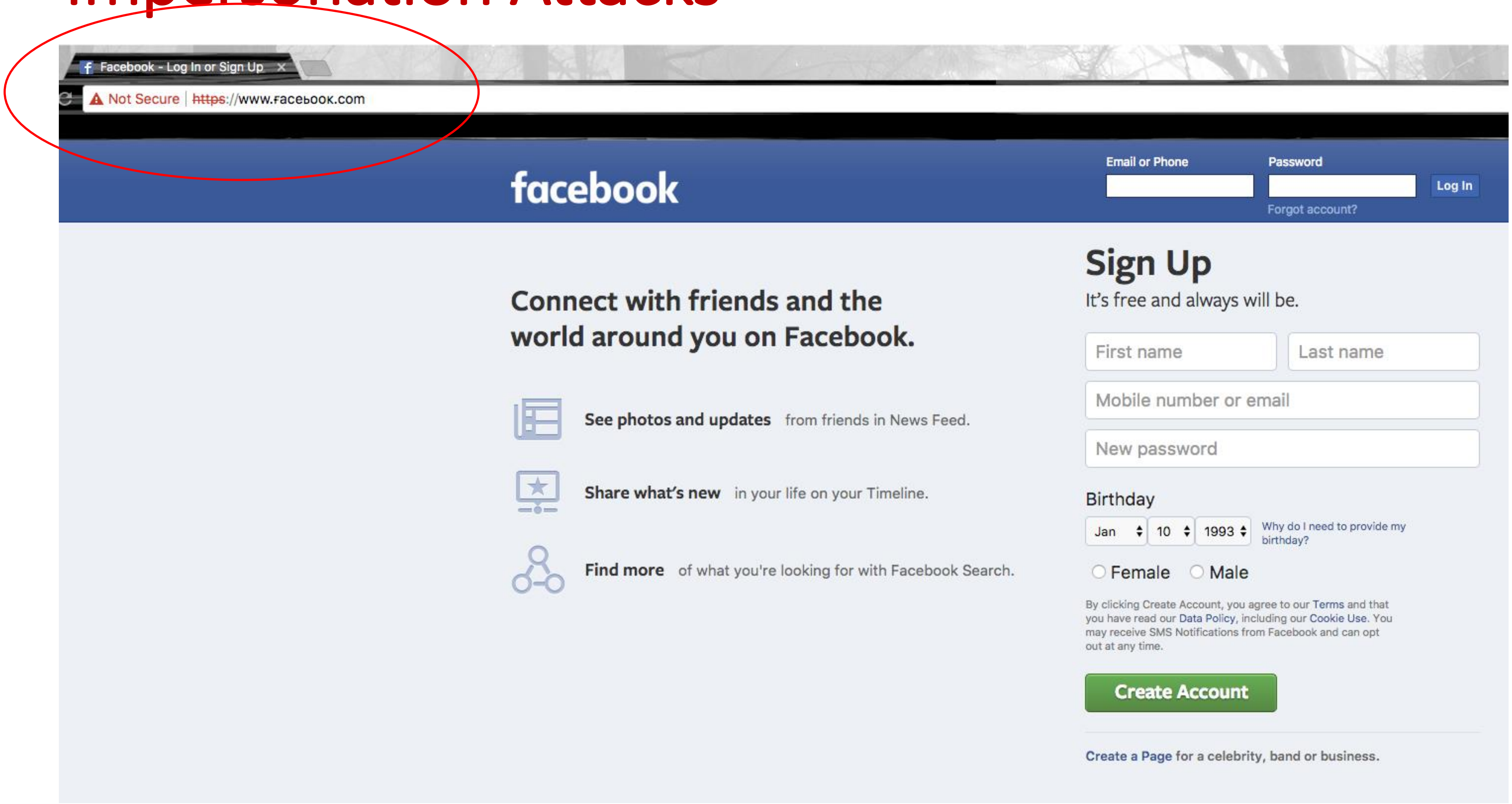
Bank of America welcomes former Countrywide customers. Your accounts are all available in Online Banking. Sign in on this page using your Username.

Let's work together to make your trial loan modification permanent.
Act now »

Products & Services	Manage Your Money	Achieve Your Goals
Checking	Online Investing	**Investment Services**
Savings & CDs	Order Check Card	Merrill Lynch
Credit Cards	Facts About Fees	Plan for Retirement
Mortgage UPDATED	**Online Banking »**	Keep the Change®
Refinance	View Your Accounts	Add It Up™ Cash Back
Home Equity	Bill Pay	Financial Education
Auto Loans	Use Mobile Banking	Student Banking
Insurance & Protection	Track Your Expenses	
IRAs		

http://www.techjaws.com/fake-bank-of-america-website/

Impersonation Attacks



Facebook - Log In or Sign Up
Not Secure | ~~https~~://www.ғacebook.com
facebook
Email or Phone
Password
Log In
Forgot account?

Sign Up

It's free and always will be.

Birthday

By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any time.

Create a Page for a celebrity, band or business.

Connect with friends and the world around you on Facebook.

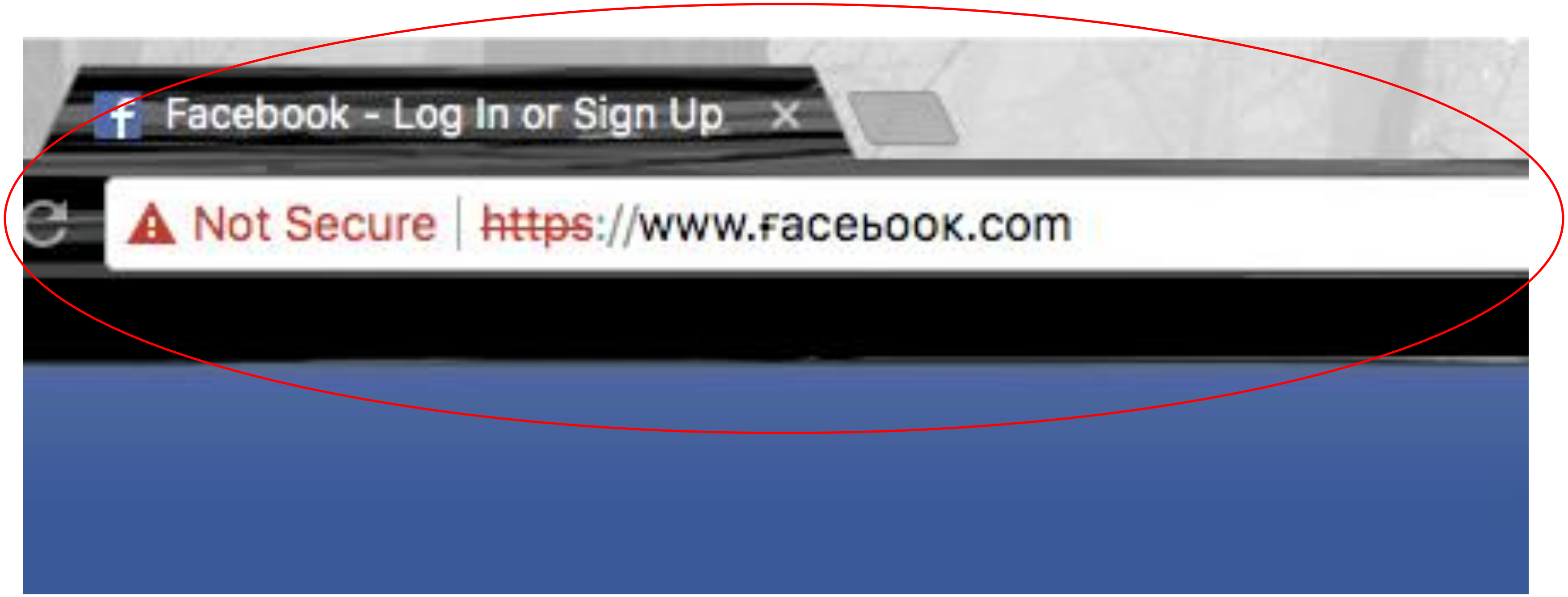
See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

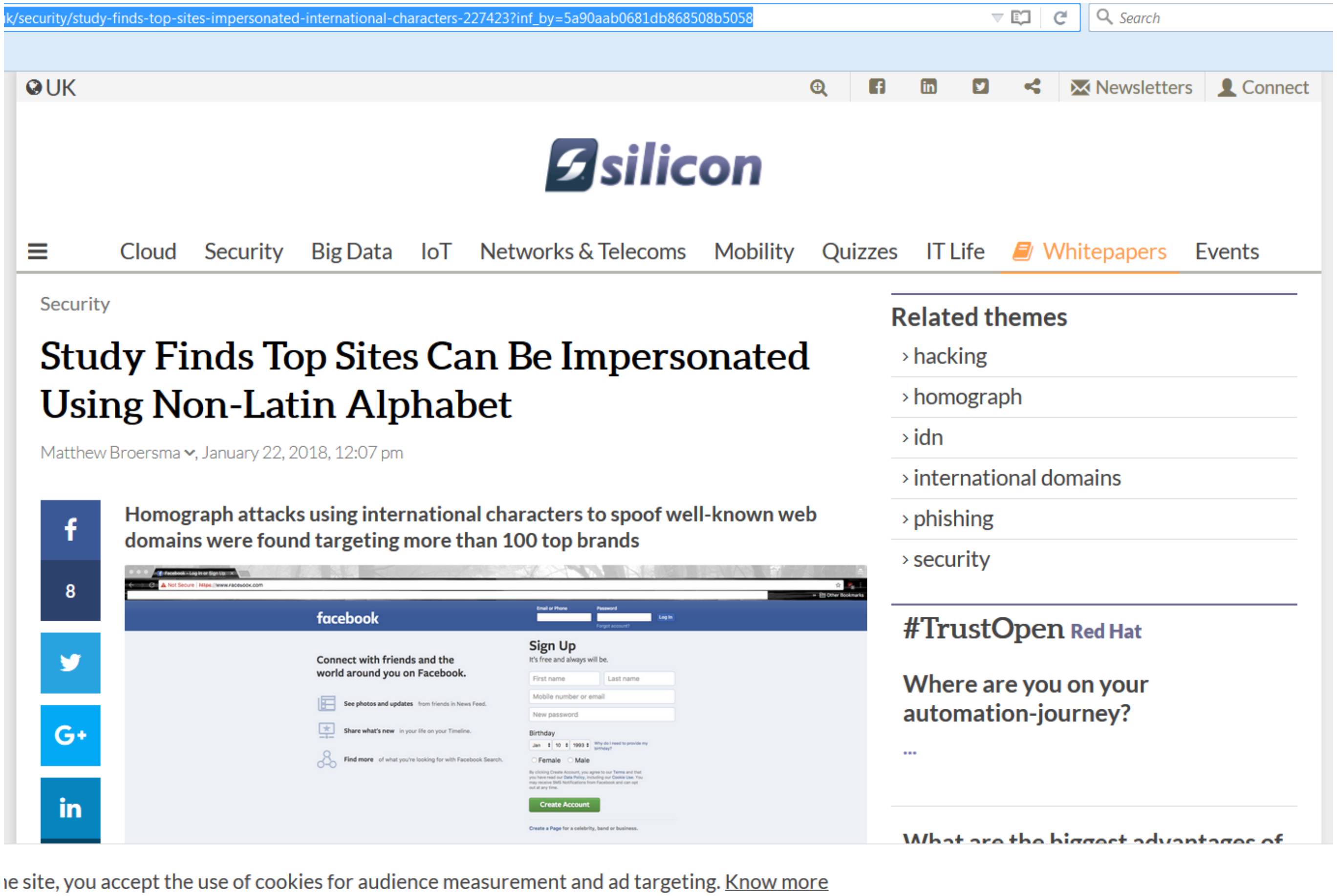
http://www.silicon.co.uk/security/study-finds-top-sites-impersonated-international-characters-227423?inf_by=5a90aab0681db868508b5058

Impersonation Attacks



⚠ Not Secure | ~~https~~://www.ғaceьooк.com

http://www.silicon.co.uk/security/study-finds-top-sites-impersonated-international-characters-227423?inf_by=5a90aab0681db868508b5058



k/security/study-finds-top-sites-impersonated-international-characters-227423?inf_by=5a90aab0681db868508b5058

UK

Newsletters Connect

silicon

Cloud Security Big Data IoT Networks & Telecoms Mobility Quizzes IT Life Whitepapers Events

Security

Study Finds Top Sites Can Be Impersonated Using Non-Latin Alphabet

Matthew Broersma, January 22, 2018, 12:07 pm

Homograph attacks using international characters to spoof well-known web domains were found targeting more than 100 top brands

8
facebook
Connect with friends and the world around you on Facebook.
Sign Up
It's free and always will be.
Create Account

Related themes

- hacking
- homograph
- idn
- international domains
- phishing
- security

#TrustOpen Red Hat

Where are you on your automation-journey?

...

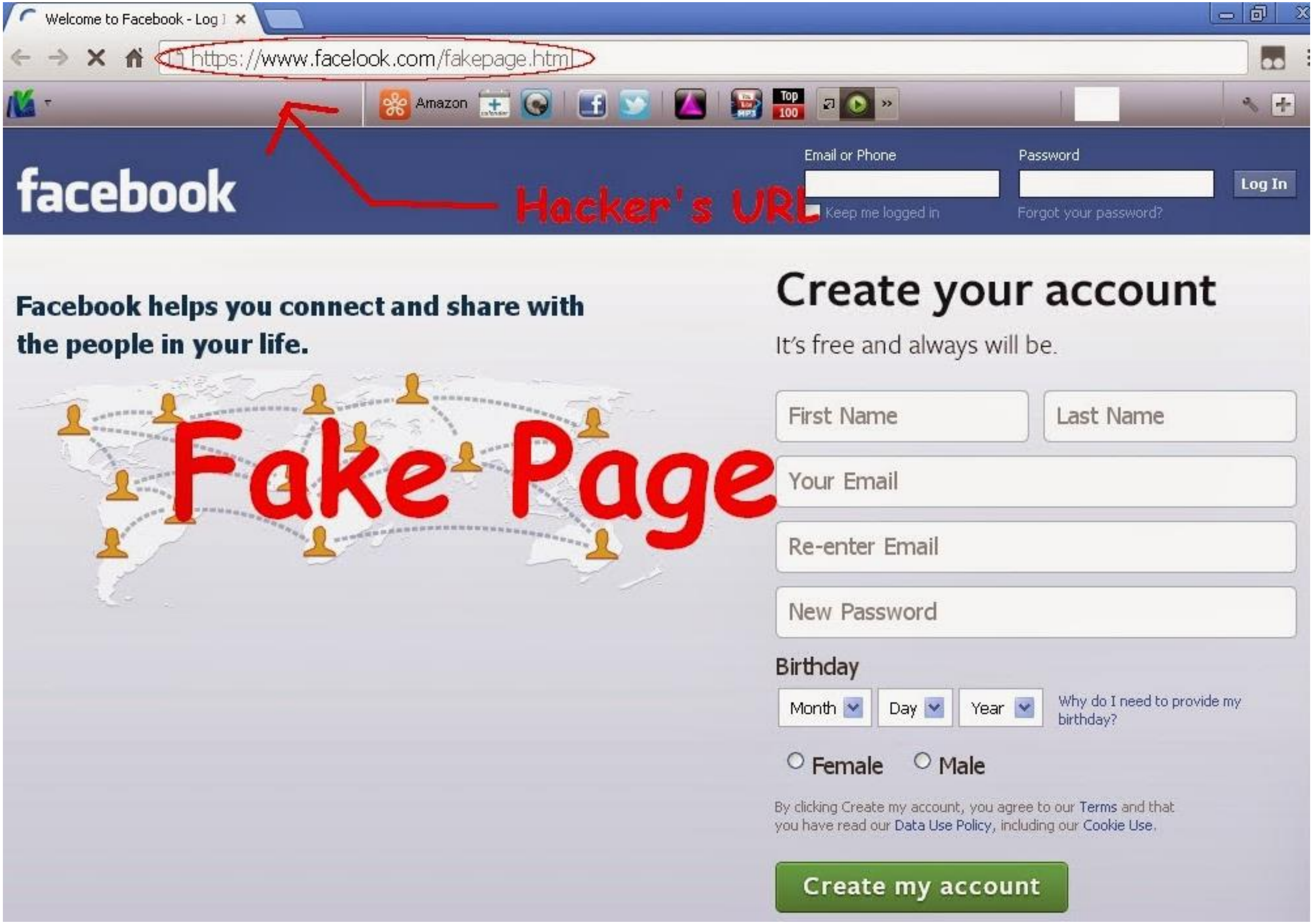
What are the biggest advantages of

ıe site, you accept the use of cookies for audience measurement and ad targeting. Know more

Phishing Attacks Prevention

- How can user protect itself?
  - Check URL!
    - URL may be similar looking, but different spelling/typo
      - Facelook.com instead of Facebook.com
    - International alphabet may be used instead
      - Looks like original English address, but different
  - Check links before clicking by hovering over them
    - Actual link may be different than displayed text

http://ehindistudy.com/2016/06/21/what-is-url-in-hindi/
https://www.viglink.com/blog/2012/05/21/hyperlinks-are-dumb-and-bleeding-money-how-to-ensure-yours-arent/



Welcome to Facebook - Log I

https://www.facelook.com/fakepage.html

Hacker's URL

facebook

Email or Phone

Password

Log In

Keep me logged in

Forgot your password?

Facebook helps you connect and share with the people in your life.

Fake Page

Create your account

It's free and always will be.

First Name

Last Name

Your Email

Re-enter Email

New Password

Birthday

Month | Day | Year

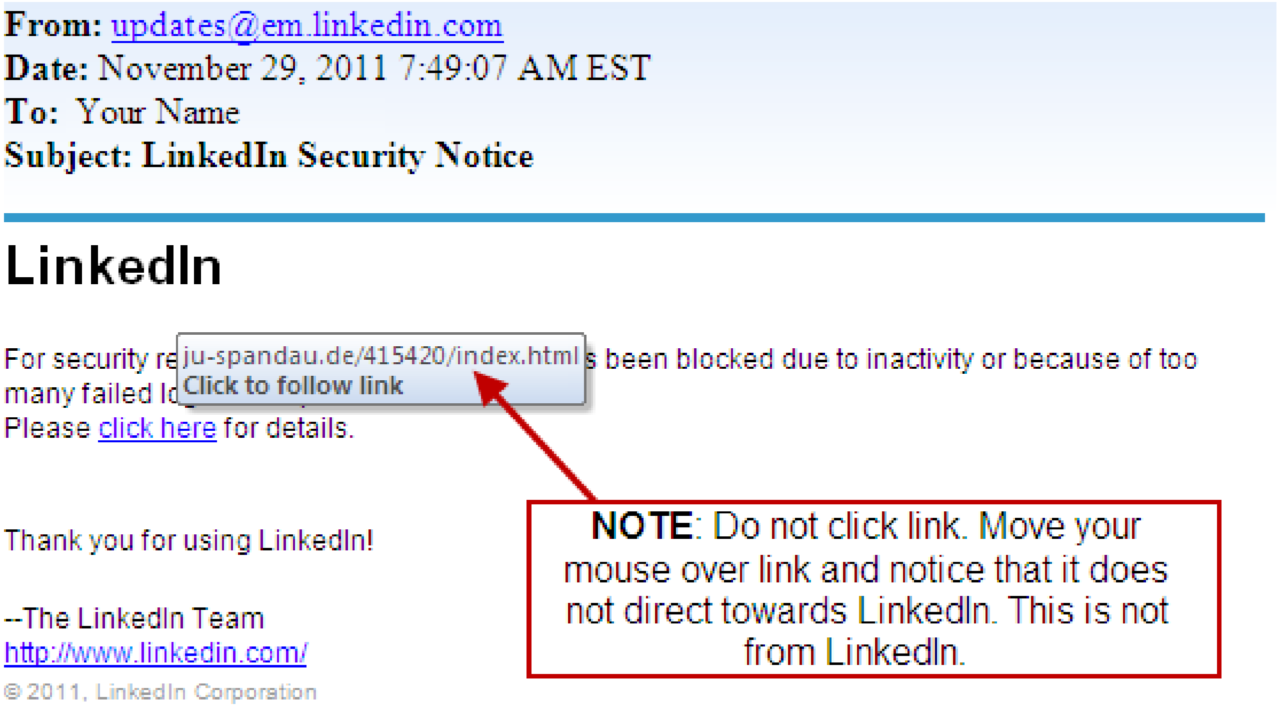
Why do I need to provide my birthday?

○ Female ○ Male

By clicking Create my account, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Create my account

http://subkuch2.blogspot.com/2013/12/how-to-hackers-hack-facebook-account.html



From: updates@em.linkedin.com
Date: November 29, 2011 7:49:07 AM EST
To: Your Name
Subject: LinkedIn Security Notice

LinkedIn

For security re ju-spandau.de/415420/index.html s been blocked due to inactivity or because of too many failed lo
Click to follow link
Please click here for details.

Thank you for using LinkedIn!

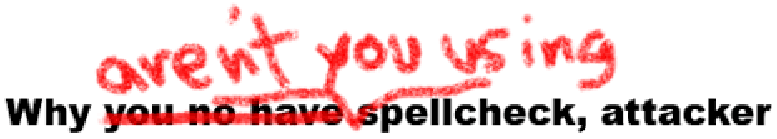
--The LinkedIn Team
http://www.linkedin.com/
© 2011, LinkedIn Corporation

NOTE: Do not click link. Move your mouse over link and notice that it does not direct towards LinkedIn. This is not from LinkedIn.

https://gburt94900.weebly.com/section-6--effects-of-using-ict/phishing

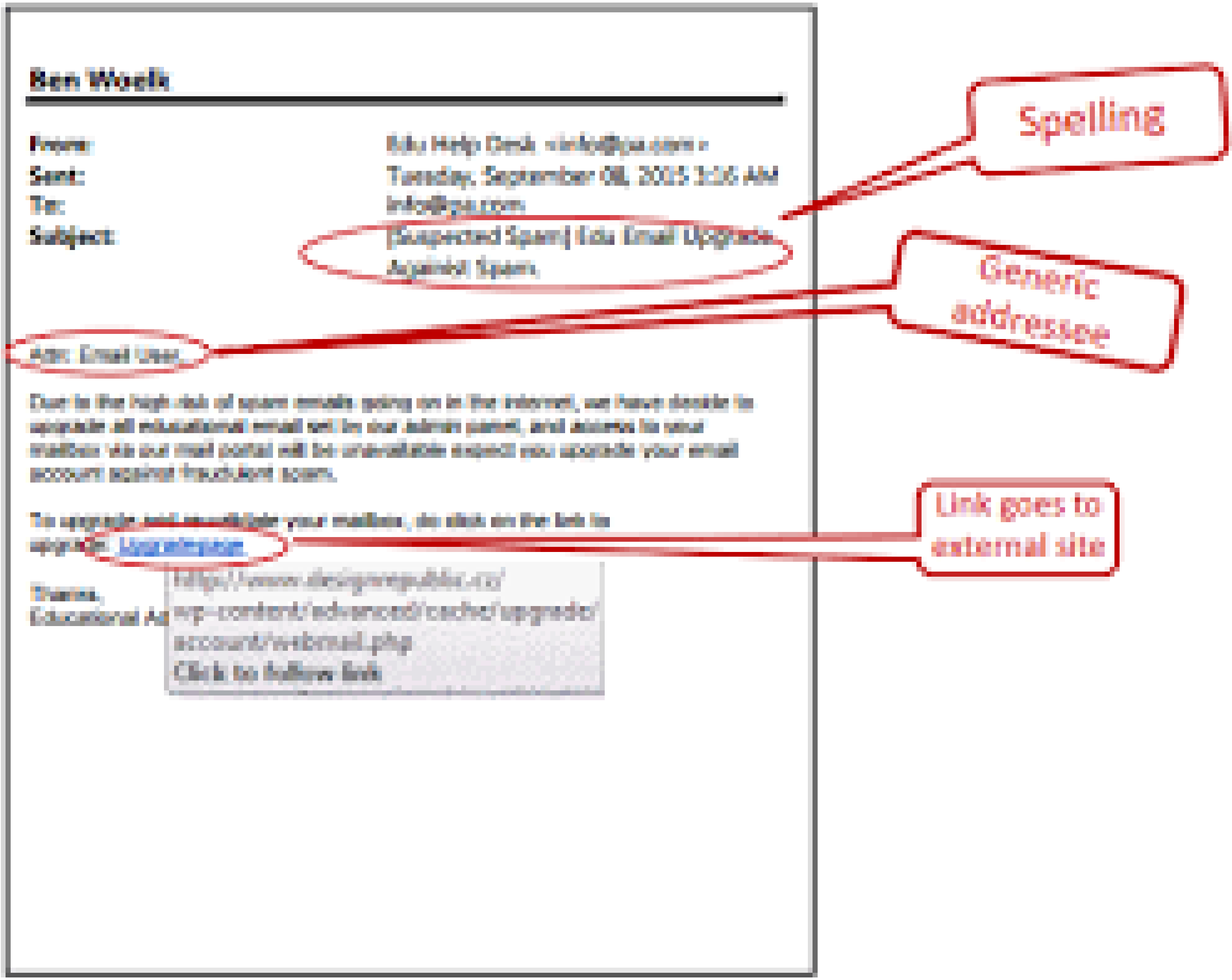
Phishing Attack Prevention

- Other warning signs to look for:
  - Spelling mistakes
  - Generic links or email addresses, e



Why ~~you no have~~ aren't you using spellcheck, attacker

https://umbrella.cisco.com/blog/2016/02/08/grammar-and-spelling-errors-in-phishing-and-malware/



Ben Woelk

From: Edu Help Desk <info@jpa.com>
Sent: Tuesday, September 08, 2015 3:16 AM
To: info@jpa.com
Subject: [Suspected Spam] Edu Email Upgrade Against Spam.

Attn: Email User,

Due to the high risk of spam emails going on in the internet, we have decide to upgrade all educational email set by our admin panel, and access to your mailbox via our mail portal will be unavailable expect you upgrade your email account against fraudulent scam.

To upgrade and revalidate your mailbox, do click on the link to upgrade: Upgrade now

Thanks,
Educational Ad

http://www.designrepublic.cz/wp-content/advanced/cache/upgrade/account/webmail.php
Click to follow link

Spelling

Generic addressee

Link goes to external site

https://www.rit.edu/security/content/how-spot-spear-phishing-attack

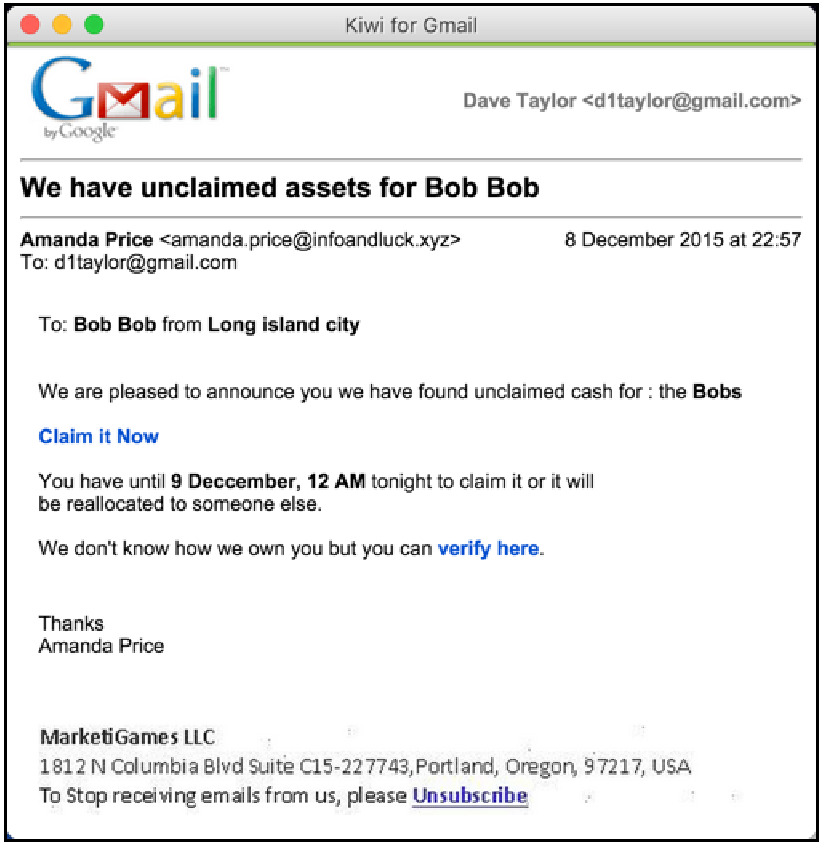
Spear-phishing

Spear-Phishing

- More sophisticated phishing attack
- Targeted towards a specific individual, organization or business
  - Uses information about target to lure him
    - Gain his trust
  - intended to steal data for malicious purposes
    - Typically for financial gain
    - Data may be used for ID theft

https://www.maketecheasier.com/spear-phishing/

Spear-Phishing Attack -Example



Dave Taylor <d1taylor@gmail.com>

We have unclaimed assets for Bob Bob

Amanda Price <amanda.price@infoandluck.xyz> 8 December 2015 at 22:57
To: d1taylor@gmail.com

To: **Bob Bob** from **Long island city**

We are pleased to announce you we have found unclaimed cash for : the **Bobs**

Claim it Now

You have until **9 Deccember, 12 AM** tonight to claim it or it will
be reallocated to someone else.

We don't know how we own you but you can **verify here**.

Thanks
Amanda Price

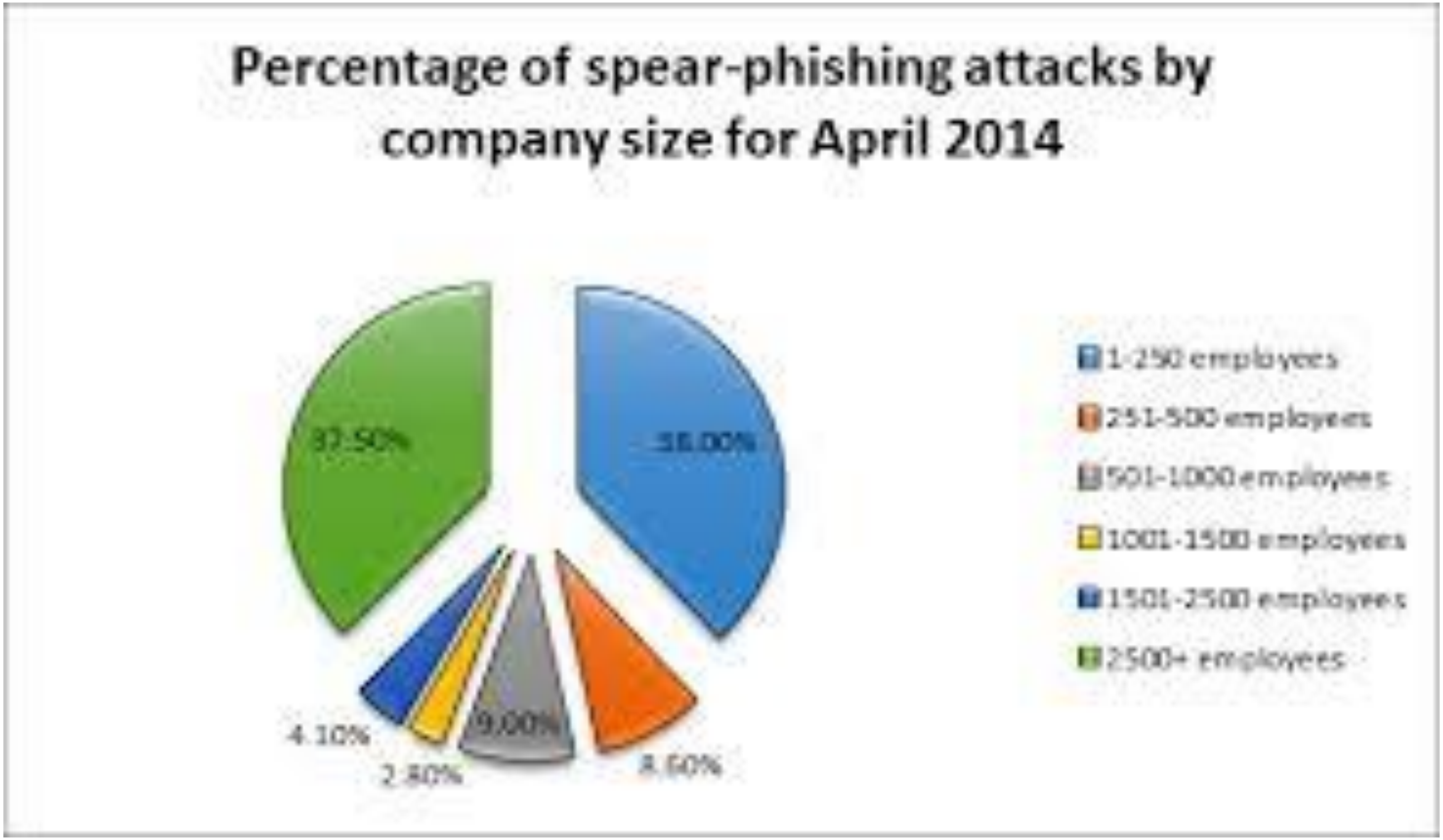
MarketiGames LLC
1812 N Columbia Blvd Suite C15-227743,Portland, Oregon, 97217, USA
To Stop receiving emails from us, please Unsubscribe

https://www.askdavetaylor.com/what-is-spear-phishing/

Spear-Phishing Attack -Example

- In this email, the attacker uses the target name and city (Long-Island)
  - Provides the target with a false sense

Spear-Phishing Attacks



http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/#gref

Spear-Phishing Attacks

- Mostly large and small companies targeted
- Why smaller companies?
    - May have weaker online security
    - rely on cloud services some of which lack strong encryption mechanisms
    - May become a luring entry point for further attacks on its larger clients
    - Many small businesses exist
        - 28 million small businesses in the US (2014)

Spear-Phishing Attacks

- Large companies are also frequently targeted
  - Large amounts of sensitive data,
  - If attack successful, attack gains fame
  - 5 out of 6 large companies attacked by phishing

http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/#gref

Spear-Phishing Attacks Statistics

- How effective are spear-phishing attacks?
- 95 percent of attacks on enterprise networks are result of successful spear phishing!
- 30 percent of phishing messages get opened by targeted users
    - 12 percent of those users click on the malicious attachment or link
    - Similar number received in multiple experiments

https://blog.returnpath.com/13-spear-phishing-stats-to-build-your-case-for-email-fraud-protection/

Spear-Phishing Attacks Statistics

- Victims are reluctant to report email response
  - Only three percent of targeted users report malicious emails to management
- Email attack scams have cost companies over two billion in the past two years
  - Cost of cybercrime and data breaches expected to rise to $2.1 trillion by 2019

Phishing Attacks

- Why are they successful?
  - Explore users’ weakness
  - Uses social engineering techniques
  - Internet used to communicate with outside world
    - Risks are hard to understand
    - Responding is easy
  - Risks are rare per individual
    - Damage is typically to organizations

Phishing Prevention - Summary

- Users need to authenticate the server
  - Check the URL/address bar
  - Load the site by typing its address into address bar
    - Save to a bookmark for future use
  - Avoid clicking on links or attachments
    - From unknown sources

Phishing Prevention – Other Tools

- Mail servers also have phishing filters
    - To guard users
        - But may remove authentic emails by mistake
- Browsers receive blacklists regularly
    - New attackers will not be identified immediately
        - Limited protection against new attacks

Summary

- As web browsers have become a primary focus of users and taken on greater functionality, they've become a focus of many types of attack
- Browser and website weaknesses are often the result of some form of poor authentication
- Many attackers focus on tricking users with fake websites, misleading applications, and phishing emails
- On the server side, injection attacks are a key concern, and countermeasures to prevent them are critical

- Questions?