



Email Safety

Steve Andrews – Southwest Kansas Library System

Email Security Basics

- Email data is encrypted when transmitted (*In Flight*) via TLS
- Email data is commonly unencrypted on receiving email server or client (*At Rest*) unless specifically provisioned otherwise.
- Assume that everything you send via email can be read by anyone (*clear text*)!

PII - Personally Identifiable Information

- Any data that can be used to identify someone
- All information that directly or indirectly links to a person is considered PII
- Name, email address, phone number, bank account number, and government-issued ID number are all examples of PII
- A library card with a patron's name is PII

Phishing

- In phishing attacks, the malicious actor pretends to be someone legitimate to obtain your sensitive information, such as usernames, passwords, and other personal information.
- Phishers send out a high volume of fraudulent emails that look legitimate to trick the users into clicking a malicious link or downloading the attachment.
- Among all the types of email attacks, phishing attacks are the most common



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Red Flags Part 1 – Mass Attack

- Blank or generic greeting
- Misspelling, typos, unfamiliar languages
- Forged links to web sites

Red Flags Part 2 – Social Engineering

- Sense of urgency
- Suspicious email addresses
- Offer sounds too good to be true

Red Flags Part 3 – Setting the Hook

- Non-routine business requests
- Unfamiliar Sender
- Request for sensitive or personal information.
 - Passwords, SSN Number, Account Numbers, CC Info

Red Flags Part 4

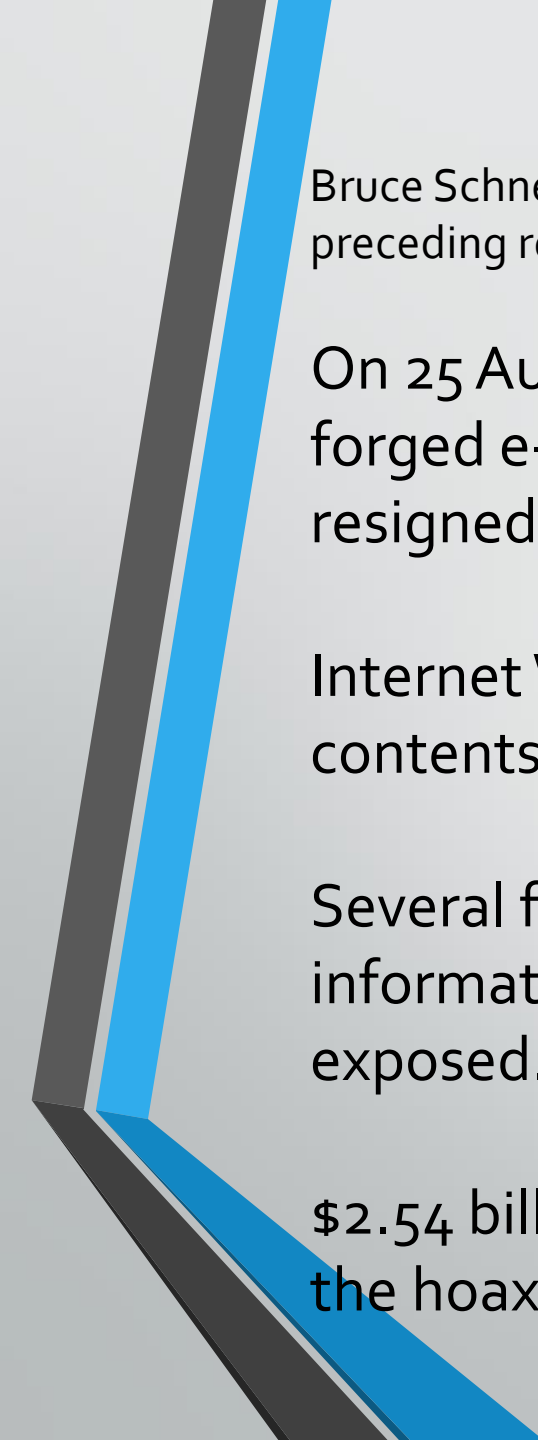
- Spoofing / Forged Sender Address



*"Only amateurs attack machines;
professionals target people."*

Bruce Schneier





Bruce Schneier, a widely respected computer security professional, privacy specialist, and writer, made the preceding remark in 2000 in an article concerning the following...

On 25 August 2000, the press release distribution service Internet Wire received a forged e-mail that appeared to come from Emulex Corp. and said that the CEO had resigned and the company's earnings would be restated.

Internet Wire posted the press release, not bothering to verify either its origin or contents.

Several financial news services and Web sites further distributed the false information, and the stock dropped 61% (from \$113 to \$43) before the hoax was exposed.


\$2.54 billion in market capitalization disappeared (only to reappear hours later as the hoax was uncovered).

Phishing Types

- Email phishing - not targeted and sent in bulk
- Spear phishing - targeted phishing attack that uses personalized emails
- Whaling - use spear phishing techniques to target senior executives and other high-profile individual
- Vishing (voice phishing) - automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts. The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution.
- Smishing (SMS phishing) - uses text messages from a cell phone or smartphone to deliver a bait message. The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.

Spear Phishing

- Why do I get more spam / phishing emails?
 - Name / email address posted on public website:
 - <https://dcpl.info/about/library-leadership/library-staff/>
 - <https://dcpl.info/about/library-leadership/library-board/>
- Name / email address contained in business listing service
- Name / email address contained in public registries (DNS, ICANN, etc.)



Fancy Bear (APT28) and the Clinton Campaign in 2016 - Spear Phishing





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

Email received by Billy Rinehart March 22, 2016



Sign-in attempt was blocked

[redacted]@gmail.com

Someone just used your password to try to sign in to your account. Google blocked them, but you should check what happened.

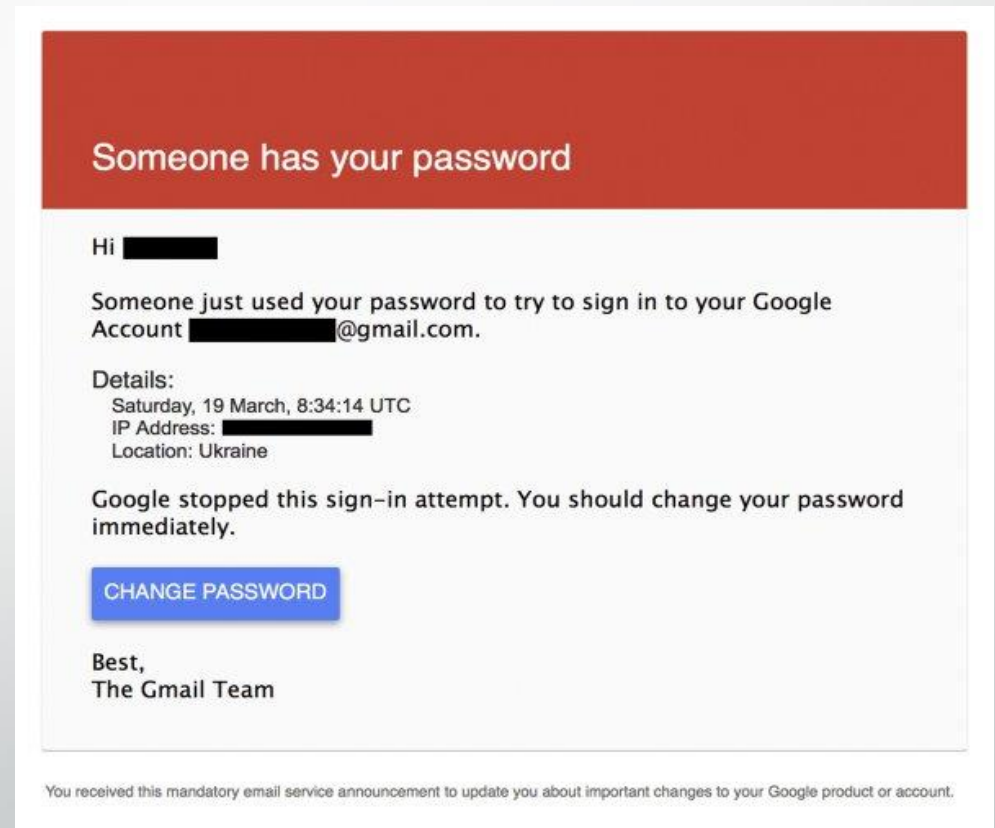
[CHECK ACTIVITY](#)

Actual Google message for blocked sign-in attempt

Fake Email Examination

- Fear – Account has been compromised
- Urgency - pressure to act immediately
- Representativeness - Made to look like the real Google alert
- Availability - Ukraine had been in the news recently
- Affect - High benefit / low risk to click link to reset password
- URL Shortener to fake webpage to reset password
- HTTP rather than HTTPS on password reset webpage

Account(s) did not have 2FA / MFA enabled.



Give Yourself a Break

- We all have bad days.
- Even the most security-aware individuals can miss phishing red flags if scanning messages quickly.
- Take the time to read and react to every incoming email appropriately.

Phone a Friend

- When in doubt, ask a colleague to look at a suspicious email with you
- Contact the person that supposedly sent the email
- Contact SWKLS I.T. Department to help examine the email

Never...

- Provide sensitive information / PII to anyone in an email (yours or patron)
- Communicate login information or passwords in an email
- Re-Use the same password for your email account on another online account
- Open an attachment unless you know who it is from & are expecting it
- Click links within an email unless you are absolutely sure they are safe
- Use business email for personal use and vice versa

Always...

- Use two-factor / multi-factor authentication for your email accounts
- Create a strong password for your email account
- Slow down and read the email entirely
- Look for clues that something is not right about the email
- Be extremely careful with attachments in emails
- Hover over links to reveal the destination URL

Resources

- <https://staysafeonline.org/resources/security-awareness-episodes/>
- https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing-es.pdf
- <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/phishing>
- <https://staysafeonline.org/theft-fraud-cybercrime/phishing/>
- <https://www.bulkorder.ftc.gov/>