ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH

2022-23

INDORE

Topic :- PHISHING

Enrollment No- 0827CI201069

Submitted to:-
Prof. NIDHI NIGAM

Submitted by:-
GOURAV CHOUHAN


PHISHING
don't get hooked

OBJECTIVES

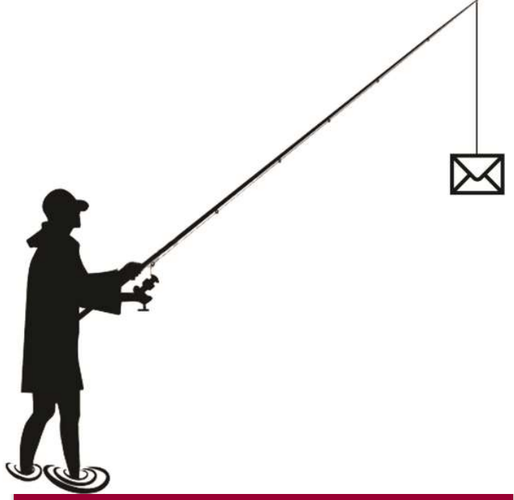
- ✓ Define phishing and identify various types of phishing scams
- ✓ Recognize common baiting tactics used in phishing scams
- ✓ Examine real phishing messages
- ✓ Understand how to protect yourself from being hooked by a phishing scam

History

- In 2004 the first Phishing lawsuit was filed in California against a 17-year-old who had constructed a false copy of a well known website, “America Online”.

- In creating this fake website the young man was able to obtain credit card details from users, which he then used to withdraw money from their accounts.

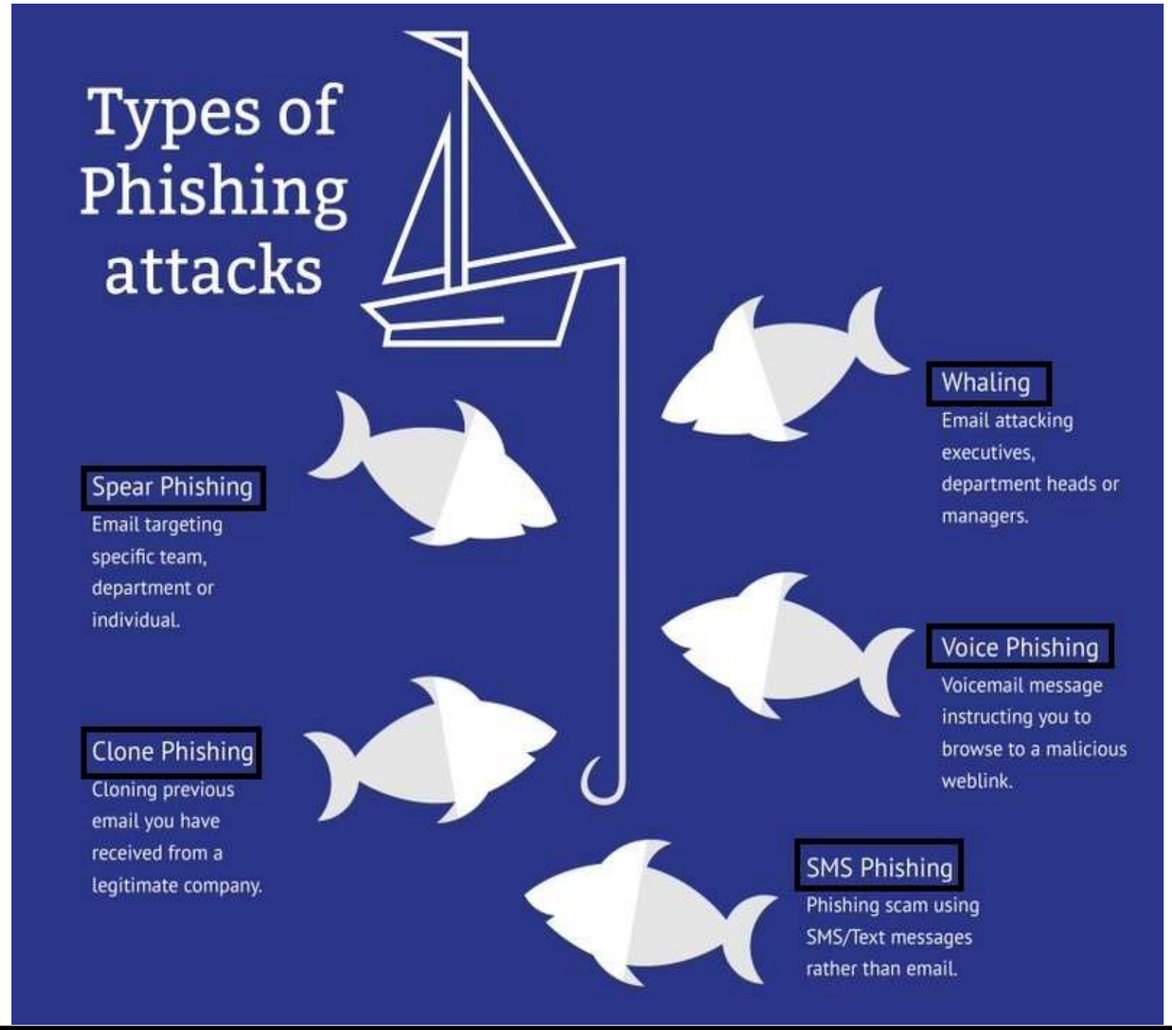
Introduction



- Phishing is a cybercrime where individuals are targeted via email, text messages or phone calls in order to retrieve private information.

- Information acquired can be passwords, documents pertaining to identification, or credit cards and banking information.

Types Of Phishing Attacks



Phone calls

- “Vishing” (Voice Phishing) is the telephone version of Phishing.

- This method of Phishing aims to verbally coerce a user into revealing sensitive information, with most cases ending in identity theft.

Text Messages

- Text Message Phishing is also known as “Smishing” (SMS Phishing).

- When a “phish” occurs, cybercriminals send deceptive messages that attempt to persuade individuals into clicking harmful links or opening malicious attachments.

“Smishing” seeks to accomplish these tasks yet use text messaging platforms as a medium.

Examples of “Smishing”

Do any of these texts seem suspicious?

Email

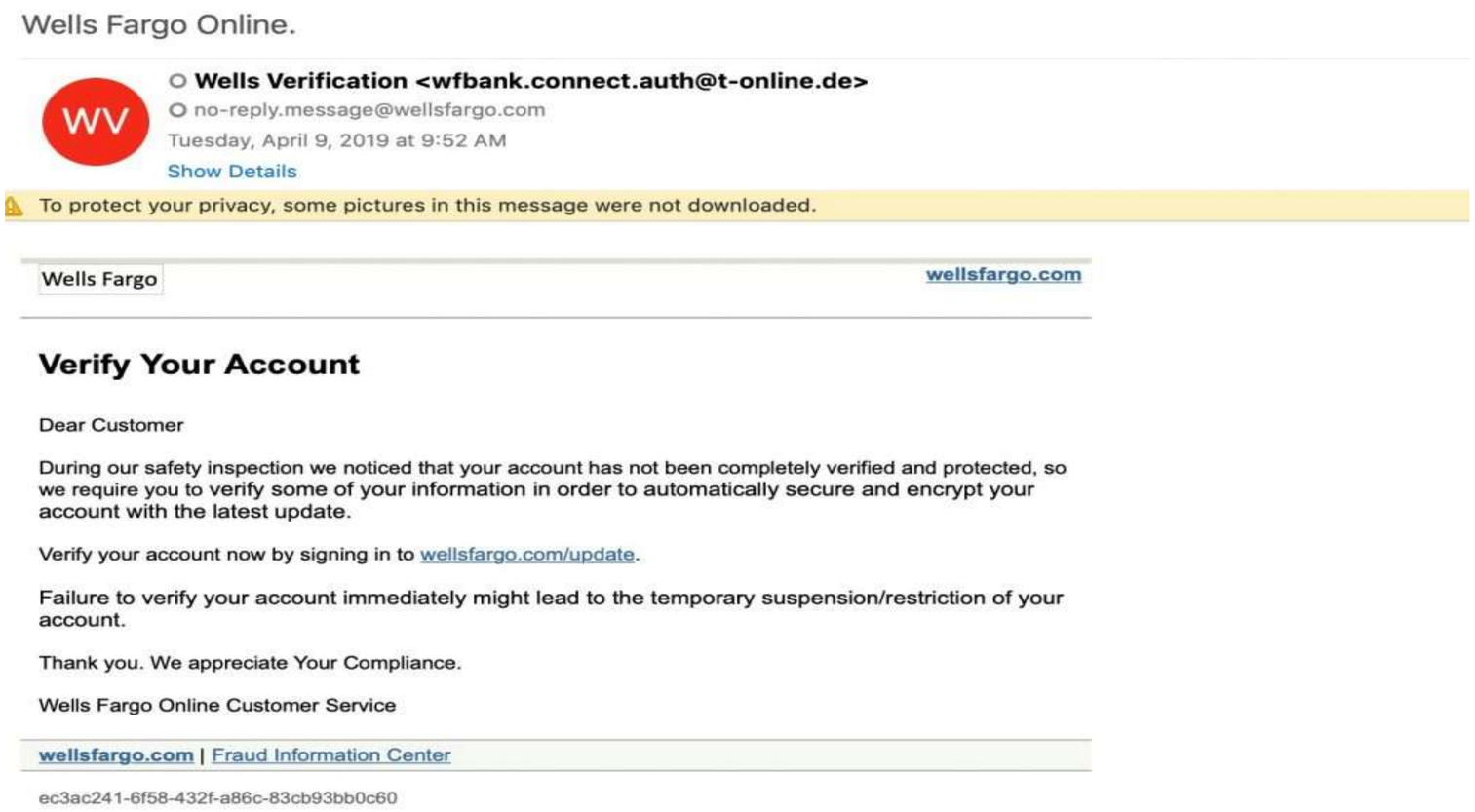
Common signs of a Phishing email are:

- Unidentified senders.
- When the email seems too good to be true.
- There is a sense of urgency for the target to respond.
- Contains suspicious looking links or attachments.

Phishing scams are found commonly in emails.

Email Phishing Example

Does anything seem suspicious about this email?



Wells Fargo Online.

WV

Wells Verification <wfbank.connect.auth@t-online.de>
no-reply.message@wellsfargo.com
Tuesday, April 9, 2019 at 9:52 AM
Show Details

To protect your privacy, some pictures in this message were not downloaded.

Wells Fargo wellsfargo.com

Verify Your Account

Dear Customer

During our safety inspection we noticed that your account has not been completely verified and protected, so we require you to verify some of your information in order to automatically secure and encrypt your account with the latest update.

Verify your account now by signing in to wellsfargo.com/update.

Failure to verify your account immediately might lead to the temporary suspension/restriction of your account.

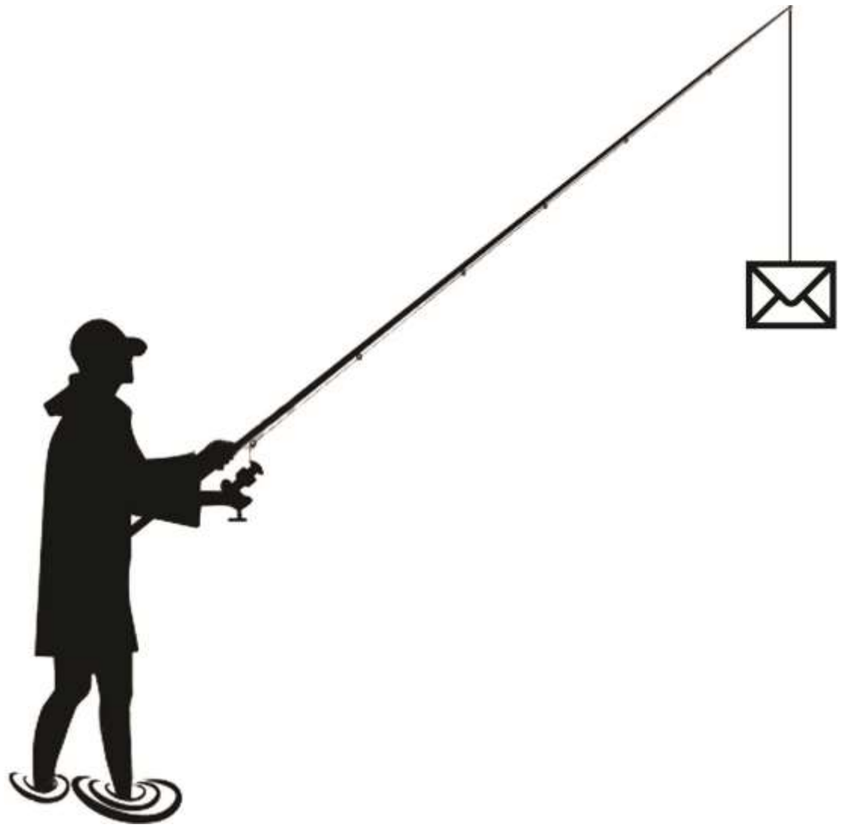
Thank you. We appreciate Your Compliance.

Wells Fargo Online Customer Service

wellsfargo.com | Fraud Information Center

ec3ac241-6f58-432f-a86c-83cb93bb0c60

How to Identify Phishing



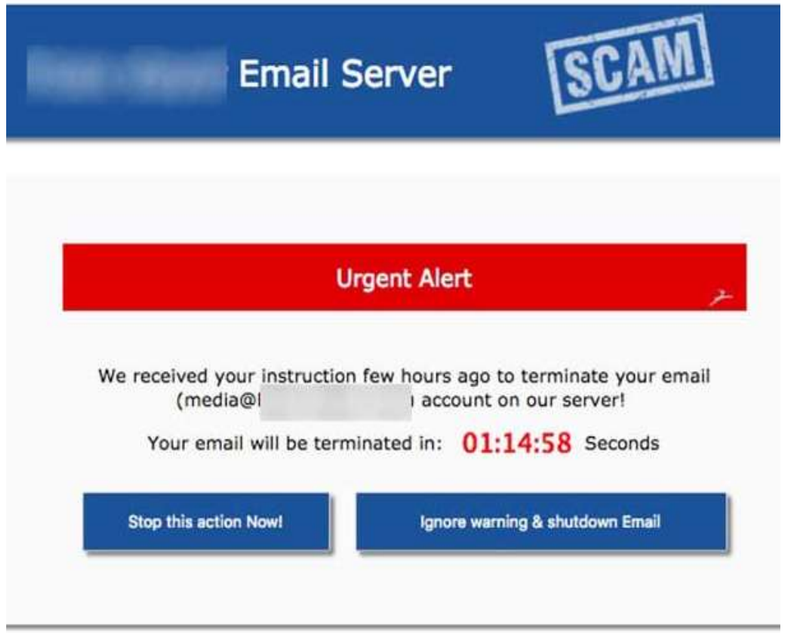
Unknown Senders

- When receiving emails be on alert for unfamiliar senders.
- Even if the email is from a known contact, be aware if the content of the email seems out of the ordinary or unexpected, it could be a scheme.

Urgency

- Some email content may pressure you to respond fast or claim that an account or subscription you hold will be suspended.

- It is beneficial to be mindful of the urgency within an email, this is a primary sign of a Phishing scam.



To Good to be True

- Phishing emails can contain promising rewards for the designated target.

- Suspicious attention-grabbing emails often guarantee the recipients that they will receive items or cash prizes.


From: Card <info@>
To: Recipients
Cc:
Subject: is giving you a chance to shop for free !

Dear Valued Customer,

is giving out free shopping vouchers for your favorites stores for Christmas.

This offer is only for Credit Card Online Services users and it will be valid to use until the 31st of December, 2013

To Qualify for this opportunity, Kindly Click here now.

After validation your voucher will be sent via text message or posted to your Mailbox.

Yours Sincerely,
Credit Card Services.

See more about: Card.

Attachments & Hyperlinks

Think before you click!

- In Phishing emails it is common to see attachments or links requesting your attention.
- Be cautious of suspicious looking links or attachments.

Prevention Measures

Preventative Measures

- Delete suspiciously “urgent” looking emails.

- Utilizing spam filters. Filters can determine the source and software used in creating spam emails. Additionally, filters may also block legitimate sources, therefore it is not completely accurate.

There are a number of ways to avoid being caught by Phishing scams.

Preventative Measures

- Change passwords regularly for accounts and never use the same password for every account.
- Utilize the number of security awareness training sessions and materials that may be available.
- Avoid using public networks when accessing sensitive information such as identification documents and banking platforms.

There are a number of ways to avoid being caught by Phishing scams.

Preventative Measures

There are a number of ways to avoid being caught by Phishing scams.

- If attachments are present, refrain from downloading suspicious documents, .txt files are the only safe file to download.

- If there are hyperlinks, hover over the URL, the link may direct to a different site completely. Pay attention to URL spelling, small changes in a valid looking link may go unnoticed.
  - Example: “google.com” vs “goggle.com”

Preventative Measures

- Configure browsing settings to avert deceitful websites from opening. Secure websites begin with “https:”. All sites will ultimately be required to have valid security protocols in place.

- Be aware that a bank will not request personal verification via email. Banks will not request an individual to update their account within a designated time period.

There are a number of ways to avoid being caught by Phishing scams.

Conclusion

- No single techonology will completely stop phishing.
- However, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it.

Refrences

- Credible Online Resources:-

  - Stay Safe Online: https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing
  - Federal Trade Commission: https://www.consumer.ftc.gov/articles/0003-phishing
  - United States Computer Emergency Readiness Team: https://www.us-cert.gov/report-phishing

THANK YOU ☺