# Social Engineering

# Social Engineering Attacks

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- Attackers generally misuse the following factors:
  - **Heightened emotions:** People are far more likely to take irrational or risky actions when in an enhanced emotional state like fear, excitement, curiosity, sadness,etc.
  - **Urgency:** People may be motivated to compromise themselves under the guise of a serious problem that needs immediate attention or may be exposed to a prize or reward that may disappear if not acted upon quickly.
  - **Trust**

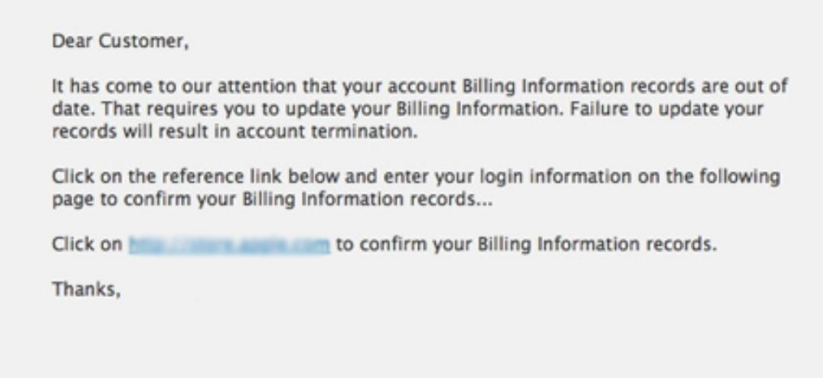
# Social Engineering Scams

| | |
|---|---|
| Investment | $8,648 |
| Romance | $6,003 |
| Moving | $3,993 |
| Cryptocurrency* | $3,147 |
| Home Improvement | $2,895 |
| Nigerian/Foreign Money Exchange | $2,133 |
| Business Email Compromise | $1,717 |
| Family/Friend Emergency | $1,219 |
| Counterfeit Product | $1,210 |
| Travel/Vacation | $887 |
| Advance Fee Loan | $716 |
| Charity | $708 |
| Identity Theft | $683 |
| Rental | $662 |
| Employment | $598 |
| Sweepstakes/Lottery/Prize | $547 |
| Fake Invoice | $441 |
| Credit Repair/Debt Relief | $388 |
| Online Purchase | $365 |
| Fake Check/Money Order | $341 |
| Tech Support | $255 |
| Credit Card | $231 |
| Government Grant | $218 |
| Health Care/Medicaid/Medicare | $170 |
| Scholarship | $155 |
| Utility | $106 |
| Debt Collection | $98 |
| Yellow Pages/Directory | $91 |
| Phishing | $44 |
| Tax Collection | $31 |
| Other | $746 |

Average amount lost per scam

# Phishing

- Attackers attempt to gain sensitive information or spread malware through fraudulent messages
    - **Spam Phishing:** non-personalised mass attack



Dear Customer,

It has come to our attention that your account Billing Information records are out of date. That requires you to update your Billing Information. Failure to update your records will result in account termination.

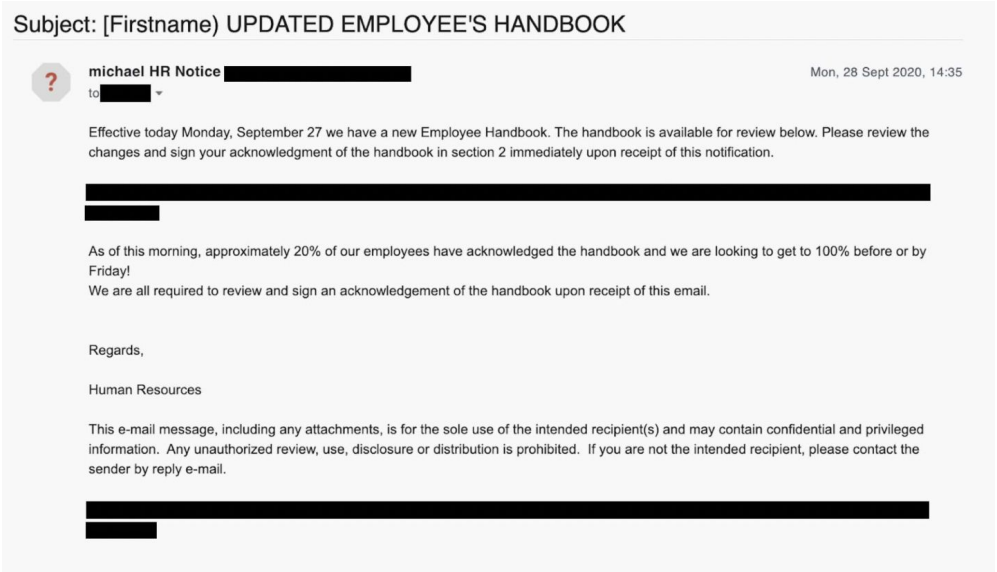
Click on the reference link below and enter your login information on the following page to confirm your Billing Information records...

Click on [redacted] to confirm your Billing Information records.

Thanks,

# Phishing

- **Spear Phishing:**personalized attacks that target specific individuals or companies



Subject: [Firstname) UPDATED EMPLOYEE'S HANDBOOK

**michael HR Notice** [redacted]
to [redacted]

Mon, 28 Sept 2020, 14:35

Effective today Monday, September 27 we have a new Employee Handbook. The handbook is available for review below. Please review the changes and sign your acknowledgment of the handbook in section 2 immediately upon receipt of this notification.

[redacted]

As of this morning, approximately 20% of our employees have acknowledged the handbook and we are looking to get to 100% before or by Friday!
We are all required to review and sign an acknowledgement of the handbook upon receipt of this email.

Regards,

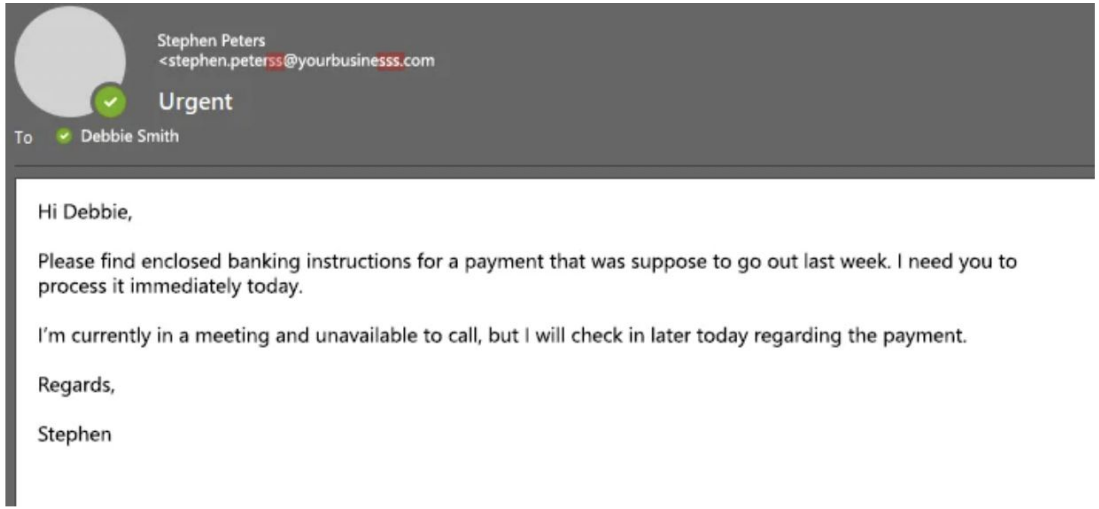
Human Resources

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail.

[redacted]

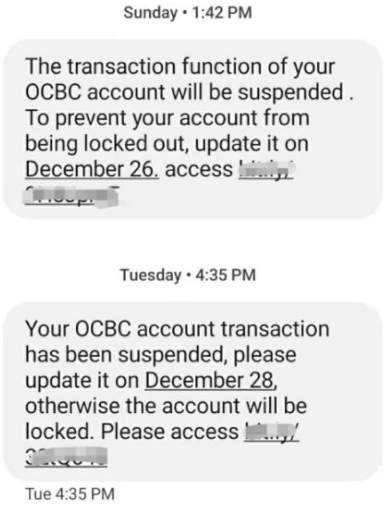
# Phishing

- **Whaling:** Targeting high-value users



# Phishing

- **Vishing:** voice phishing
- **Smishing:** SMS phishing



# Present and Future of phishing

- Earlier, it was easy to detect a phishing email (mainly because of bad grammar and typos)
- Later, the attackers copied the message content from authentic messages
- Now, the phishing messages are more customized
- Attackers gather personal information from social media
- Attackers also come up with new scams frequently

# Signs of a phishing scam

- The links or URLs provided in emails are not pointing to the correct location or are pointing to a third-party site not affiliated with the sender of the email.


- Includes request for personal or financial information.
- Includes  email address that is similar enough to a legitimate email address
- The message is unexpected and unsolicited.
- The message or the attachment asks you to enable macros, adjust security settings, or install applications. Normal emails won't ask you to do this.
- The message contains errors, typos.
- The website looks familiar but there are inconsistencies

# Social Psychology

- This discipline attempts to explain how thoughts, feelings, and behaviour of individuals are influenced by the actual, imagined, or implied presence of others
- It is important to consider this while designing operational security
- Getting employees of an organisation to resist attempts by outsiders to trick them into revealing secrets, whether over the phone or online, is known in as **operational security** or **Opsec**.

# Social Psychology

1. People generally try to conform to a group
    - People could be induced to deny the evidence of their own eyes in order conform to a group
    - Sometimes people think that it is easy to just follow others instead of voicing own opinion
    - Fear Of Missing Out (FOMO) also plays a role in decision making
    - This factor is also widely used in marketing
2. People generally obey orders of higher authority even if they do not fully agree with it
    - This can be used by fraudsters to trick their victims
3. People may abuse authority if there is no accountability

# Social Psychology

- Never train the users in such a way that it can be misused by the attackers
- People are uncomfortable when they hold conflicting views. They seek out information that confirms their existing views and try to reject information that conflicts with their views
- Admitting that you were duped can be painful

# Using human abilities for security

- There are tasks that human brain can do much better than computers
- Humans can easily recognise/identify other humans visually
- We are good at general image recognition
- We are good at understanding speech, especially in noisy environments
- These are not easy for computers
- We can use this asymmetry for our benefit

# CAPTCHA

- Completely Automated Public Turing Test to Tell Computers and Humans Apart
- Early versions set out to use a known ‘hard problem’ in AI such as the recognition of distorted text against a noisy background.
- Many of the image recognition problems posed by early systems turned out not to be too hard at all
- Google has developed reCaptcha that uses advanced approach, incorporating image based captchas using real-world images and analyzing user behavior to distinguish between human users and bots.

# Authentication

- Authentication can be done using
  - Something you have: Key fob, id card, token generator, authenticator apps ...
  - Something you know: PIN, password, ...
  - Something you are: Fingerprint, iris, ...
  - Something you do: Handwriting, Voice pattern, etc
- Required strength of the passwords vary depending on the application
- For better security, we can use multi-factor authentication that combines two or more of the above techniques

# Concerns related to Passwords

- Remembering passwords:
  - The password problem can be summed up as “choose a password you can’t remember and don’t write it down”

- Reliable password entry: user may not be able to enter the password correctly if
  - the password is too long or complex
  - there is no clear visibility of the input device
  - user is under stress

# Concerns related to Passwords

- User may break the system by disclosing the password to a third party either accidentally, on purpose, or as a result of deception
  - Naive password choice
  - User abilities and training
  - Design errors
    - Interface design: Example: Keyboard in ATM, CCTV cameras near the keyboard
    - Eavesdropping: Example: Public Wi-fi
    - Visible indication of wrong password even before completing the password entry. Example: Timing Attack
  - Attack on stored passwords: Where and How to store the password is crucial

# Possible Attacks

- Brute force attack
- Offline Dictionary Attacks/Rainbow table attack
- Specific Account Attack
- Popular password Attack
- Exploiting user mistakes
- Exploiting repeat password use
- Electronic monitoring

# Countermeasures

- Using strong passwords/passphrases
- Storing passwords in browsers
- Password manglers
- Password managers
- Soft keyboards
- Two-factor/Two-channel authentication (with full transaction details)
- Trusted Path:  some means of being sure that you're logging into a genuine machine through a channel that isn't open to eavesdropping.
- Creating awareness

# References


1. https://www.kaspersky.co.in/resource-center/definitions/what-is-social-engineering
2. https://www.youtube.com/watch?v=4o5hSxvN_-s
3. https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf
4. https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/phishing?view=o365-worldwide
5. https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html