PEOPLE: THE NEGLECTED FACTOR IN CYBER SECURITY

Mohammed Shafiul Alam Khan

PhD (Information Security, RHUL, UK)

Professor, Institute of Information Technology (IIT)

University of Dhaka

Email: shafiul@du.ac.bd

Outline

- Overview of a Security System
- Different Class of Security Attacks
- What to Do and What Not to Do
- Conclusion

Overview of a Security System

People

Process

Technology

All three of these combined, protects any system from threats and attacks.

The People

- **People** are the weakest link to security programs (most neglected factor).
- Technology and processes are mostly reliable.
- Human being are unpredictable, susceptible to attacks and can be stressed into doing something out of protocol.
- **Human error is still the greatest cause of data breaches and security failures** (Source: Helpnet Security).
- A single human error is enough to bring down the whole system

Security Attacks

Social Engineering Attacks

- ❑ **Social engineering attack** uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- ❑ Attacker needs **valid data** to trick users.
- ❑ **One need to know how attacker collect data for social engineers attacks.**

Gathering Information for Social Engineering Attacks

Gathering Information

- A staggering wealth of information exists in online databases, public records, and social media sites, and in many cases, this data is free for the taking.
- Human intelligence is data gathered by **talking to people**.
- Google hacking

Different Social Engineering Attacks

Pretexting Attack

- Attackers use information to pretend to be a trusted entity to a specific user.
- Create scenarios where the user is convinced to trust them
- Finally, give up sensitive information and perform activities that render the user vulnerable.

Example

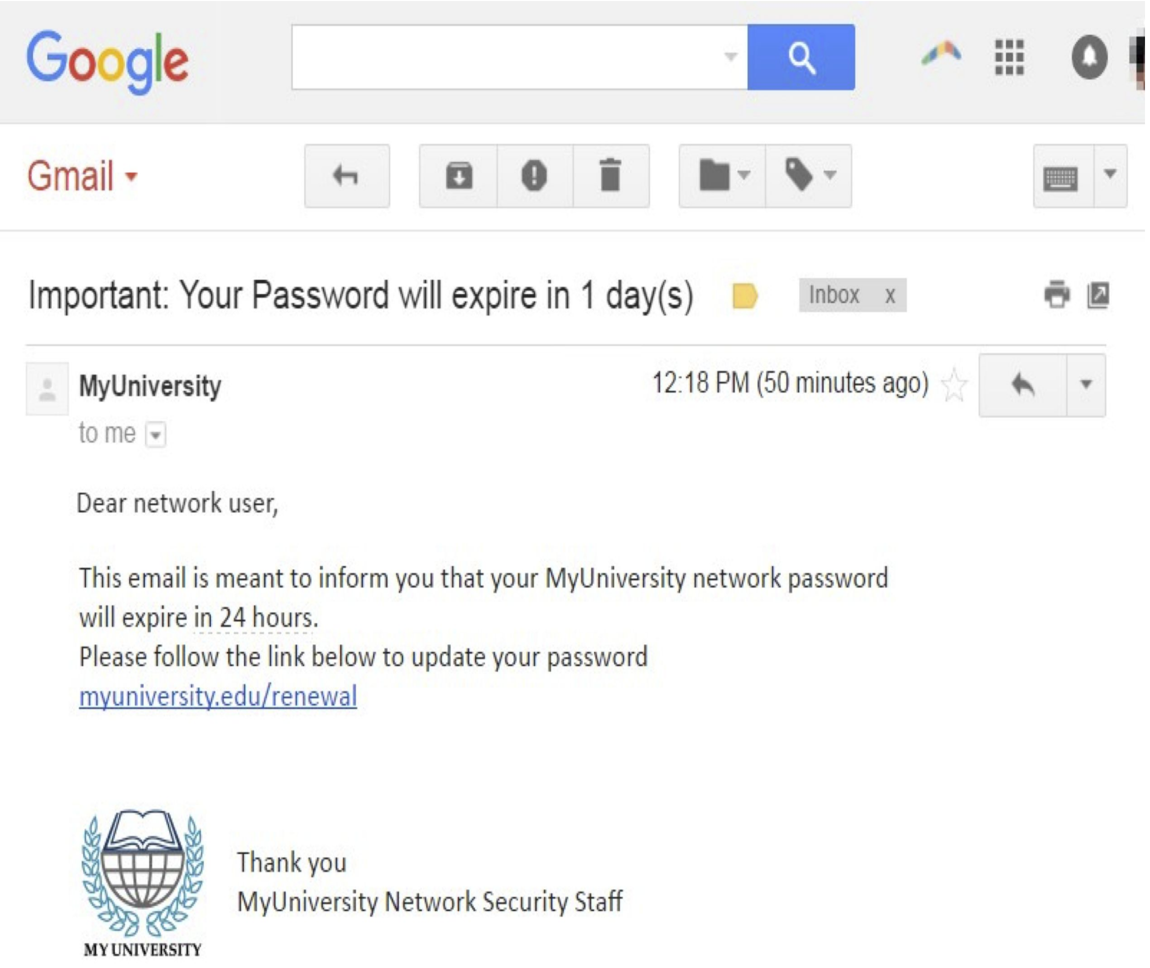
Assume someone calls an employee and pretends to be someone in power, such as the CEO or on the information technology team.

The attacker convinces the victim that the scenario is true and collects information that is sought.

Phishing Attack

- Attacker uses electronic communications such as email, texting, or phone calls to **convince** the target to click a malicious link.

- Goal is to collect the target's **personal information** or **install malware** on their system.



Important: Your Password will expire in 1 day(s)

MyUniversity
to me

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

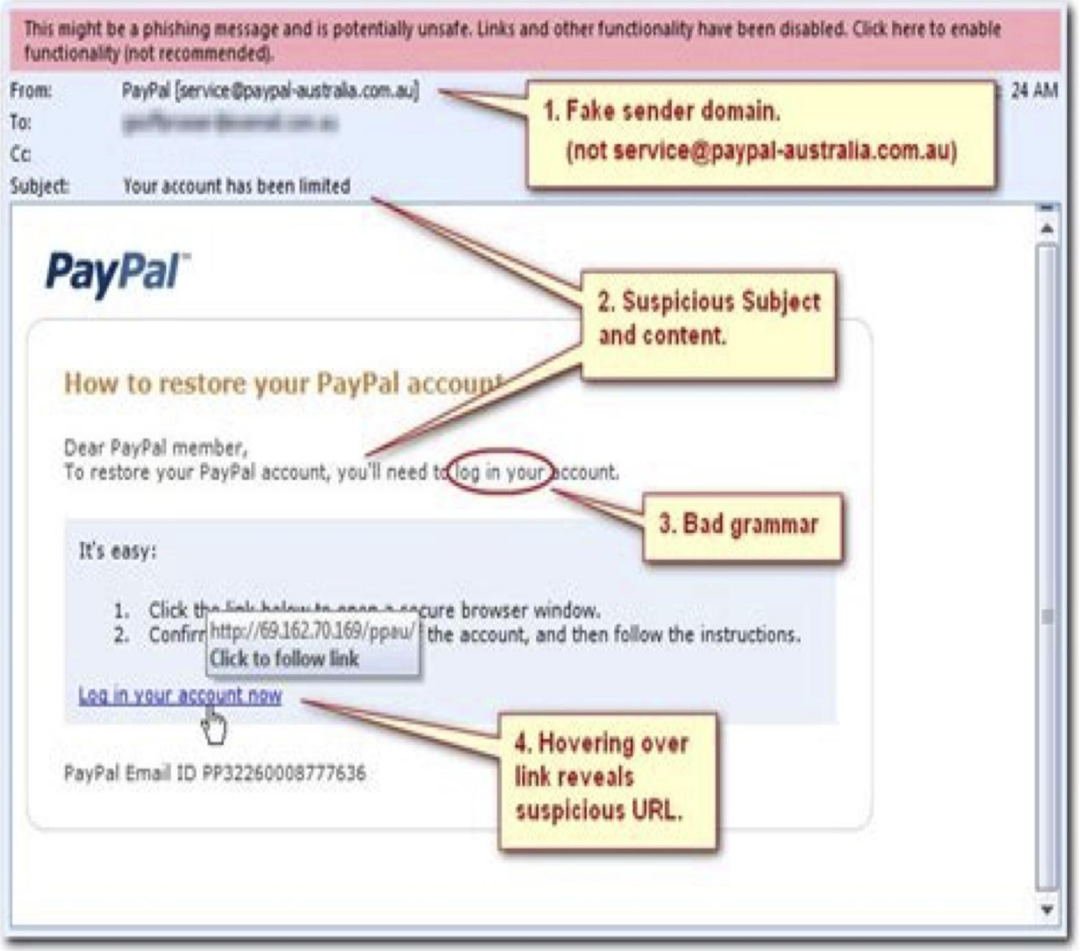
Thank you
MyUniversity Network Security Staff

Phishing Attack – An Entry Point for Attacker

- **Phishing accounts for 37% of all cyber-attacks directed toward businesses.**
- More than 90% of successful attacks against businesses originate from phishing.
- 37.9% of Untrained Users fail Phishing tests
- 74% of all Phishing websites use **HTTPS (Secured HTTP) – Padlock cannot safe you!**
- 94% of Malware is delivered via email (using Phishing attack)
- A new Phishing site launches every 20 seconds

How to Tackle Phishing Attack

- Don’t click any links on an email unless you can guarantee who its from
- Look details of such an email carefully
- Use a trusted method of contacting via a phone number, or website
- Mark the email as spam
- Using updated browser



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

24 AM

PayPal

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirr the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

1. Fake sender domain.
(not service@paypal-australia.com.au)

2. Suspicious Subject and content.

3. Bad grammar

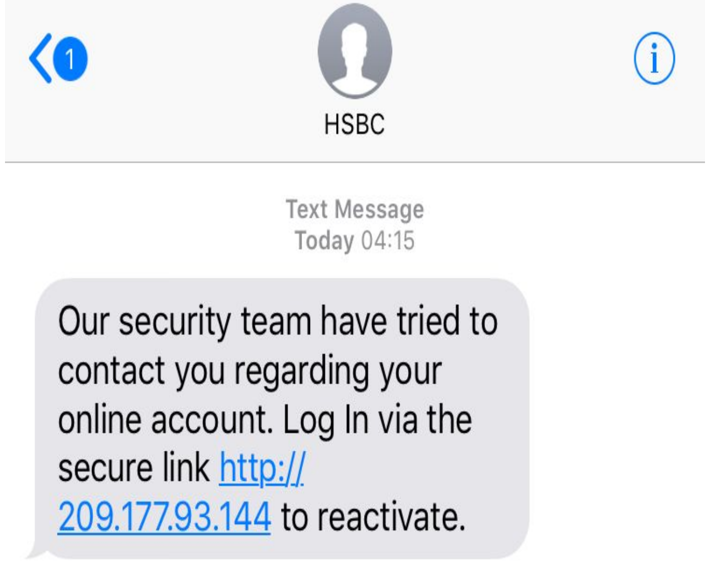
4. Hovering over link reveals suspicious URL.

Vishing and Smishing Attack

- Vishing and Smishing are similar to phishing.
- Vishing is convincing a target to give access to computer over telephone.
- Smishing is sending fraudulent links over SMS to bait a victim.

How to Tackle Vishing and Smishing Attack

- ❑ Avoid responding to **text messages from strangers**. If there are any links, images or other attachments in such messages, **do not tap** them.
- ❑ Use apps like **Truecaller to identify unknown callers**.
- ❑ Never give out **sensitive data** like **bank details, passwords and credit card** details over phone calls or messages unless the recipients are people you're familiar with.



Text Message
Today 04:15

Our security team have tried to contact you regarding your online account. Log In via the secure link http://209.177.93.144 to reactivate.

Scareware

- ❑ Attackers use to scare people into downloading malicious software.
- ❑ For example, rogue scareware or fake software include Advanced Cleaner, System Defender, and Ultimate Cleaner.

Prevention

- ❑ Use software from trusted companies.
- ❑ Avoid popups and use adblocker.

Baiting

- Baiting means offering something enticing or curious in front of the victim to lure them into a social engineering trap.
- For example, encouraging a person to provide bKash PIN in exchange for free money.

Prevention

- Staying vigilant about suspicious offers.
- Conduct organized simulated attacks to check employee awareness.

Quid Pro Quo

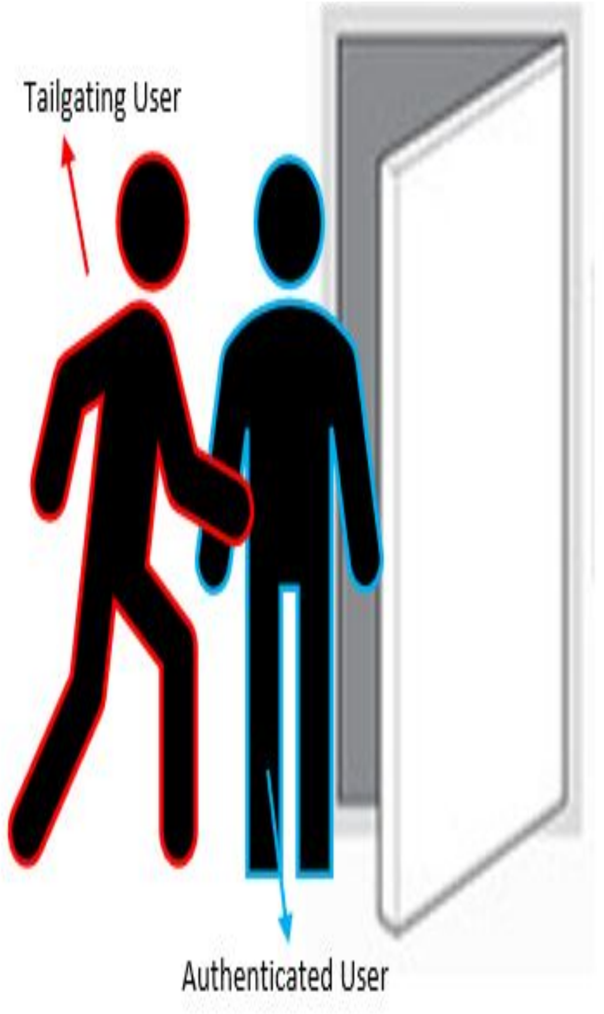
- ❑ Quid Pro Quo means something for something.
- ❑ Quid pro quo usually provides sensitive information in exchange for a service.
- ❑ For example, social media like Facebook offers free services in exchange for a ton of user data.

Prevention

- ❑ Reading privacy policies and terms and conditions before signing up for a free service.
- ❑ User Awareness.
- ❑ Remembering any free service is not always free

Tailgating

- ❑ Tailgating, or piggybacking, is the act of following someone through an access control point, **instead of using the credentials normally needed to enter**.
- ❑ For example, a user fails to properly log off their computer, allowing an unauthorized user to "piggyback" on the authorized user's session.



Prevention

- ❑ Always log off from public computers
- ❑ Avoid logging into sensitive sites using public networks
- ❑ Avoid physical tailgating through video surveillance

Building Security Awareness with Training Programs

Social Engineering Training

Training users to recognize and respond to social engineering attacks can be an incredibly arduous task because such attacks **take advantage of our behavioral norms and tendencies.**

- ❑ Users should be taught to be **suspicious** of anything that seems **unusual**
- ❑ Ask people to **trust but verify** when faced with even the slightest doubt
- ❑ Users may flood security operations center with calls and emails, but at least they won’t fall victim.
- ❑ Teach **password hygiene**
- ❑ **Create policies** regarding social engineering attacks

Passwords Hygiene

- Password breaches pose serious security risks.
- More than 3 billion passwords end up in the wrong hands each year (through Data Breach)
- The most common password is “123456.”

Not to Do

- Leaving passwords written in obvious locations
- Share them with others
- Reuse the same passcode over and over again

Passwords Hygiene

To Do

- Use 1 password per account/Service
- Use **strong passwords**: Use long passwords and combine uppercase letters, lowercase letters, numbers, and symbols.
- **Change** your password frequently**. Never reuse** passwords
- Be careful where you enter your password (**protect shoulder surfing**)
- Enable **Two-Factor Authentication** where required
- Password managers can be helpful to store your passwords
- Create policies regarding password hygiene

Use of Public Wi-Fi

- May **not be trustworthy**. They **could share your information** to other companies who operate in countries without any data protection.
- You **may not know who is watching** you whilst you're online.

What to Do and Not to Do

- Don't access sensitive application from Public Wi-Fi. Use your own data.
- Don't conduct any purchases
- Use a virtual private network (VPN)

Personal Equipment Hygiene

To Do

- ❑ Set rules for **when and how** employees can use **personal equipment** in the workplace.
- ❑ Set **guest networks** for personal equipment
- ❑ Educate employees about personal equipment **usage and the risks**
- ❑ Communicate that these **policies** apply to devices such as vendor laptops or mobile devices that can connect to networks.

Clean Desk Policies

- A clean desk policy states that **no sensitive information** should lay unattended on a desk for any significant period of time.

- Introduction of such a policy should also entail **introduction to the practice of proper disposal of physical media** containing sensitive information.

Acknowledgement

- https://datareportal.com/reports/digital-2022-bangladesh

(DataReportal is **an online reference library** offering hundreds of reports packed with data, insights, and trends)

- https://dataprot.net/statistics/cyber-security-statistics/

Any Questions?

Thank you for Listening!

For further query please contact me at

shafiul[at]du.ac.bd