

BUSINESS EMAIL COMPROMISE (BEC)



Attacker uses the identity of someone in a company or who has authority to trick its personnel into sending money to the attacker's account.

- Spoofing or compromising an email account
- Sending an email from an account to financial personnel requesting a wire transfer
- Once transfer occurs, the payment is sent to money mules and then forwarded onto cyber attackers

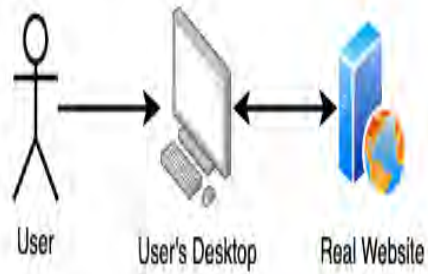
SPOT THE DIFFERENCE?

maybank2u.com is not the same
as maybank2u.com

citibank.com is not the same as
citibank.com

Man-in-the Middle (MITM) Attacks

Normal Scenario



MITM Attack



Makes it possible for an attacker to eavesdrop on the data sent back and forth between two networks

Attacker positions themselves in the “middle” or between the two parties trying to communicate.

The MITM illicitly modifies or accesses the message before it reaches its destination.

Some ways to protect yourself and your organization from MITM attacks is by using strong encryption on access points or to use a virtual private network (VPN).

PASSWORD ATTACKS

Do not keep passwords on pieces of paper or sticky notes

Social engineering used to convince you to input your password to solve an "important" problem.

A brute-force password hack uses basic information about the individual to try to guess their password.

A dictionary attack uses common words and phrases to try and guess the target's password.

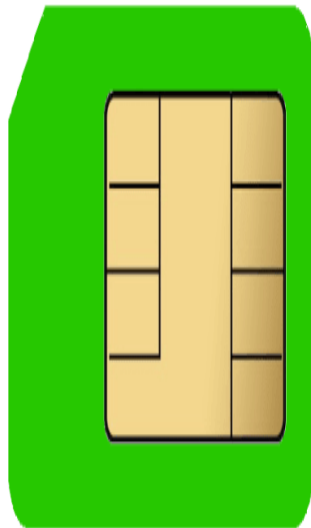
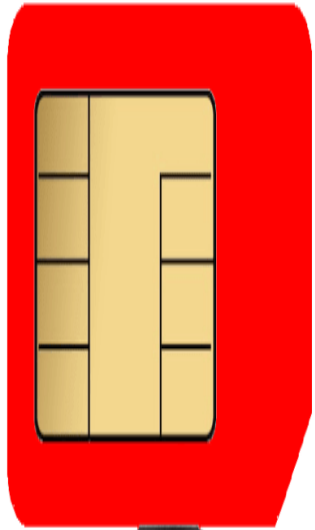
One effective method of **preventing brute-force and dictionary password attacks** is to **set up a lock-out policy.**



Brute Force Password Timeline

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

SIM Card Swapping



Scammers contact your mobile phone's carrier and trick them into activating a SIM card that the fraudsters have, or utilize access inside a cell phone provider to have the SIM card swapped

Once this occurs, they have control over your phone number. Anyone calling or texting this number will contact the scammers' device, not yours.

If you're a victim, you won't be able to make calls or send texts

Consider using a Two-Factor Authentication App rather than your cell phone for accounts



Challenges



- Cyber attackers test their malware against off-the-shelf security products
- Cyber attackers will target personal devices and home computers
- Sophisticated malware will likely get past your security software and could get installed on your devices
- A well organized and executed social engineering campaign is highly effective in tricking victims to provide private information or clicking on a link

What can you do? Individual Cyber Hygiene

Update/patch systems
Multifactor Authentication
**Virtual Private Network
(VPN)**
Password Manager Tool
Encryption Applications
Mobile Device applications
Social media



Other Personal Tips & General Best Practices

- **Back up your data**
- **Change passwords (every 45 to 90 days).**
- **Do NOT give out your usernames, passwords, etc.**
- **Delete and do NOT open emails, links, or attachments from unknown/suspicious sources**
- **Do NOT connect to unsecure/public Wi-Fi or hotspots**
- **Monitor financial accounts daily**
- **Do NOT conduct sensitive activities (online shopping, banking, or sensitive work) using a public wireless network or publicly accessible computer**
- **Mobile network connection is generally more secure than a public wireless network.**

