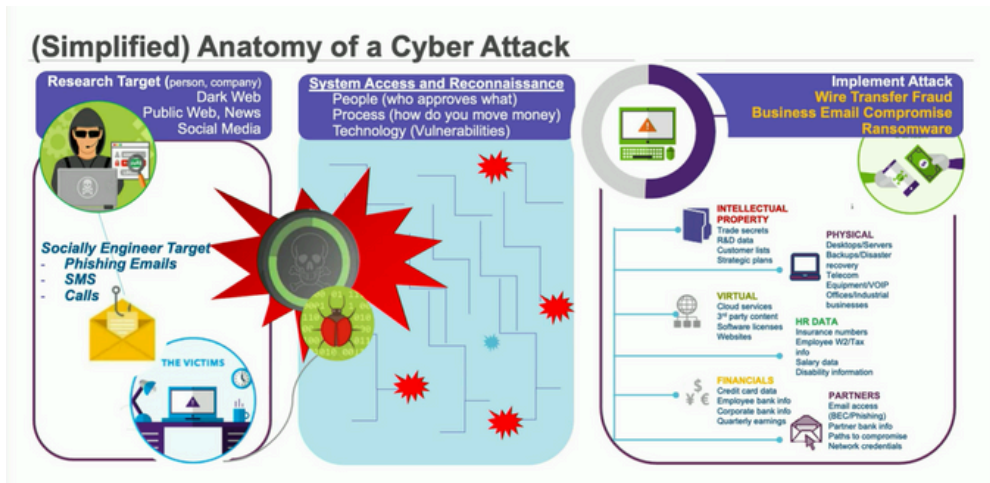


HELPFUL TIPS



In today's world, one cannot be too safe.



The top method of all successful Cyberattacks start with Phishing

Uber Hack: It's the Simple Things That Kill Your Security

Regarding its recent hack, Uber blamed the largest hacking group for its security breach. Experts had also breached Microsoft, Cisco, Samsung, Nvidia, and Oracle, among others.

Phishing Attack

The original compromise appears to have been when the contractor was tricked by a phishing attack into giving up his user ID and password. Still, since his Uber account was protected by multifactor authentication (MFA), it still should have been OK.

Right? Right!? Wrong.

Eventually, the contractor accepted an MFA request, and the attacker was in. People, come on! If you get an MFA request you don't recognize, you don't approve it!

Successful hacks that started with phishing or passwords for sale....

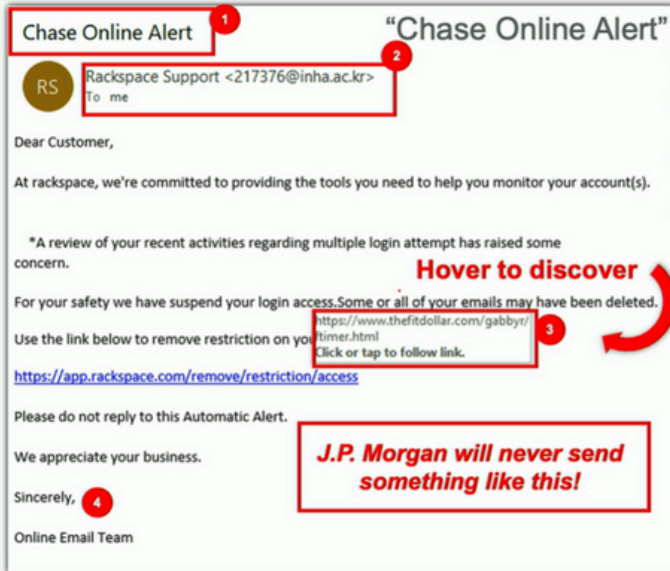
- Microsoft
- Cisco
- Samsung
- Nvidia
- Okta
- Uber
- American Airlines.
- Sequoia Capital.
- etc.

American Airlines learns breach caused by phishing

September 26, 2022

Even if you trust— VERIFY

You are the best and most effective cyber defense



Signs of a Phishing email

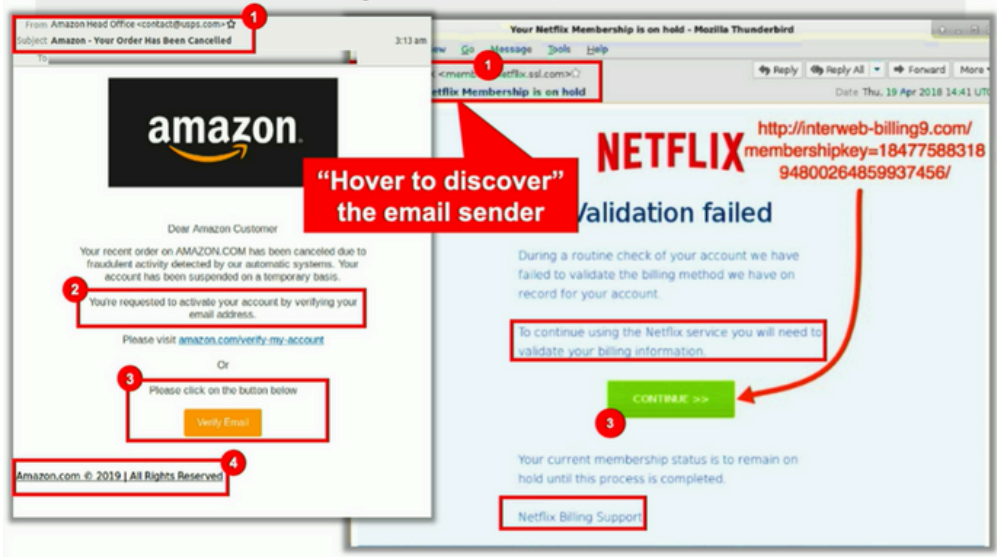
- 1 There is not a Chase logo
- 2 The message is sent from a fake email domain
- 3 Suspicious attachments or links
- 4 Email is poorly written and could contain spelling and grammar issues

Does the email make sense from the senders email?

Is there a way to contact Customer Service?

Would I normally send information via a link I cant identify?

Phishing Examples: "Your Netflix Membership is on hold"; "Your Order has been cancelled"



Phishing Email Signs

- 1 The message is sent from a fake email domain
- 2 Email creates a sense of urgency
- 3 Suspicious attachments or links
- 4 Email is poorly written and could contain spelling and grammar issues

When in doubt
Verify, Verify, Verify

Secure your online accounts

Enable two factor authentication whenever offered!



Strengthen the security of your online accounts

- Enable two-factor authentication wherever offered
 - Banking, email, social media, shopping, airline, and mobile service provider accounts
- Turn on login alerts to warn of any suspicious activity
- Use strong and complex passwords

Passwords

Do you have a password that looks like this?

Top 10 Most Hackable Passwords

123456	password	admin	princess	qwerty
123456789	letmein	Baseball	iloveyou	football

Hackers can crack 2/3 of all passwords

Passwords

Creating strong passwords

Passwords should be:

- **Longer**, not shorter – use a song, **phrase**, book title, more characters is better (8 is not enough!)
- **Complex**, not simple – upper- and lower-case; numerals and special characters
- **Not written down** – not on a sticky note, not in a spreadsheet and not in contact “notes”