**3010 Week 9 Tutorial: Honan Case Study & Phishing**

(Related to Matt Honan Get hacked Article-Answers all within article)

1. Give a simple 1-2 statements on How did Matt Honan various accounts get hacked at the same time?

His accounts were daisy chained together and he did not use 2FA for his Google account. Amazon let hackers get into his Apple ID account which helped them get into Gmail and gave them access to Twitter.

All his accounts were chained together

1. How did Apple tech support gave the hackers access to Matt iCloud account?

They issued a temporary password after the hacker claimed to be Matt.

Just his email address and the partial 4 digit credit card number

1. What piece of information did Amazon give to the hacker that enables them to convince Apple that the hackers can claim Matt’s identity?

Last 4 digits of credit cards for an account

1. What kind of problem is this?

Identity Verification Problem

Data Management

1. Did the hacker answer correctly the security questions? If no, then how did they convince Apple they are Matt?  
   No, The hacker provided only two pieces of information that anyone with an internet connection and a phone can discover.

Email address, billing address and the last four digits of my credit card

1. A temporary password reset was issued by Apple. How did the author Matt miss it?

The email arrived in his me.com email address which he rarely checks.

He did not check email that moment, but the hacker did and deleted immediately

1. What did the hacker do after this?

He followed the link in that email to reset Hanon’s AppleID password

1. One after another in quick succession, his various accounts were broken and passwords reset. What can we learn about this?

Different accounts on the Internet are interconnected and can leak crucial information.

Hackers work very fast to exploit such links so that we are caught unaware

1. How did his iphone, ipad, and Mac Data get wiped out?

ICloud’s Find My tool was used to remotely wipe the data.

1. What kind of background research did the hacker do on Matt?

The hacker went to find Matt’s gmail email address and the last four digits of his credit card number.

His Twitter account linked to his personal website, where they found his Gmail address. Guessing that this was also the email address he used for Twitter, Phobia went to Google’s account recovery page. Hacker did not even have to actually attempt a recovery. This was just a recon mission.

1. How did hacker find his alternate e-mail he had set up for account recovery?

Matt did not had 2FA turned on and when the hacker entered his Gmail address, he could view the alternate email Matt set up for account recovery.

1. In what other way did Google contribute to the successful hack?

Google only partially obscures the recovery email information, starring out many characters but there were enough characters available to guess, m\*\*\*\*n@me.com

1. How did hacker get matt billing address?

A whois search was done on Matt’s personal web domain to get his billing address. If someone does not have a domain, you can also look up his or her information on Spokeo, WhitePages, and PeopleSmart

1. Is it easy for hackers to get Matt or your last 4 digits of your credit card account?

Yes, these 4 digits readily available if hackers are resourceful enough

1. In one paragraph Matt wrote what he should have done. List them.

* He should regularly back up his data on his MacBook
* He should not have daisy chained two vital accounts, his Google and ICloud accounts, together.
* He should not have used the same email prefix across multiple accounts
* He should have a recovery address that is only used for recovery without being tied to core services
* He should not have used Find My Mac

1. Why is it so hard to eliminate phishing totally?

Phishing usually occurs either due to security flaws or to a lack of user awareness towards security.

* It takes only 1 employee to let his/her guard down
* Some unsure how to verify link is correct(eg US former northwest airlines website, is it northwest.com or nwa.com?)
* Some are attracted by the deals behind the forwarded link to web pages
* Some received link from close friends and assume it is secure

1. What are the more effective ways to reduce phishing incidents to almost nil?

Increase the amount of information that a user has to provide to access their accounts be it for reset or for entry. An example is to have both 2FA and personal passwords

* Walk through with employees personally to mouse over link and observe webpage it points to
* Walk through with employee personally how to google and recognize correct link to web page-if in doubt ask someone with techie
* Stick approach is useful to ensure employee takes this lapse seriously
* If link appears in group email, highlight malicious link to everyone
* Encourage employer and partners never to send link to employees. Everything in text.