Lab – What was Taken?

Objectives

Search for and read about a few recent occurrences of security breaches.

- Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

- Required Resources
- PC or mobile device with Internet access
- Security Breach Research
    1. Use the three provided links to security breaches from different sectors to fill out the table below.
    2. Search for 5 additional interesting breaches and record the findings in the table below.

Incident Date	**Affected Organization**	**How many victims? What was Taken?**	**What exploits were used? How do you protect yourself?**	**Reference Source**
Dec 2015	Neiman Marcus	Approximately 5200 victims with their username and password stolen	Other hacked websites Use unique passwords per site	SC MagazineLinks to an external site.
Between 2009 and 2015	Centene Corp.	950,000 victims and six hard drives containing their personally identifying information information	Physical access to the drives. Use credit and health care monitoring	SC MagazineLinks to an external site.
Between 2013 and 2014	University of Virginia	1400 employees' direct deposit banking information	Phishing email scam Do not open embedded email links, access the website by visiting the website directly	University of VirginiaLinks to an external site.

August 2013	Yahoo	3 billion customer accounts	Spear-phishing email Do not click on embedded links in emails.	Yahoo Breach
November 2019	Alibaba	1.1 billion pieces of user data	Data leaks on their shopping website. Make sure website is free from exploitation and bugs.	Alibaba Data Leak
June 2021	LinkedIn	700 million users' data stolen and posted on a dark web forum	API exploitation by data scraping Improve Terms and Conditions of software and counter-act any data scraping techniques that take data not seen by public.	LinkedIn Data Scrape
March 2020	Sina Weibo	538 million accounts affected with personal information	a dictionary attack when the hacker tried to match contact information with the site's address book API. Slow down repeated logins; force captchas after multiple failed logins; lock the accounts after multiple failed logins;	Sina Weibo Breach

			ask to refresh passwords regularly; monitor for suspicious activity.	
October 2013	Adobe	Hackers stole login information and nearly 3 million credit card numbers from 38 million Adobe users.	The breach occurred after attackers compromised one of Adobe's public-facing web servers Blacklisting/whitelisting IP ranges by country. Disable remote login by root. Enable fail2ban (disables IPs after so many failed login attempts) Configure firewall to only allow relevant ports inbound (e.g. ssh, sftp, https)	Adobe Cyber Attack

- Reflection

After reading about the security breaches, what can you do to prevent these types of breaches?

It is very important to use unique passwords for different services you use. Make sure that it is not predictable nor common. It is also best to avoid opening links in emails – ensuring your own cyber safety is a must. Make sure to visit websites directly because links can redirect you to malicious content.