Lab – What was Taken? (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

1. Objectives

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

1. 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.

1. Required Resources

* PC or mobile device with Internet access

1. Security Breach Research
   * 1. Use the two provided links to security breaches from different sectors to fill out the table below.
     2. Search for a few 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 | [Securityweek](https://www.securityweek.com/neiman-marcus-says-hackers-breached-customer-accounts) |
| Between 2009 and 2015 | Centene Corp. | 950,000 victims and six hard drives containing their personally identifying information i | Physical access to the drives.  Use credit and health care monitoring | [BBC](https://www.bbc.com/news/technology-35420306) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Reflection

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answers will vary. Examples: Use unique passwords, avoid opening embedded links in an email