CYBER SECURITY TALES: YAHOO! (2013)

Adapted from "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack" by Nicole Perlroth

In 2013, hackers broke into Yahoo's user account information. They found and took away private information from all 3 billion people who had Yahoo accounts. This information included people's names, when they were born, and their passwords.

The hackers were then able to use this stolen information to break into other websites and accounts that belonged to the affected Yahoo users. To fix this problem, Verizon stepped in. Verizon bought Yahoo and aided the original Yahoo team in taking additional steps to fix their security issues using Verizon's experiences and resources. They bought Yahoo and combined it with another company they owned called AOL. The two former companies were merged together into a new Verizon division called Oath.

In this case, the hackers were caught and arrested. The Department of Justice charged four men, including two Russian intelligence officers, with the breach and included 46 other charges. Three of the hackers are Russian nationals and could not be charged by the Justice Department. The one remaining man was sentenced to five years after pleading guilty to nine felony hacking charges.

The Yahoo security breach was achieved with a phishing link email sent to a Yahoo employee. Phishing scams include emails that look like legitimate messages from trusted sources, such as banks or social media apps. They try to trick you into revealing personal information like passwords or credit card details. This breach shows the importance of using good judgment before clicking links from unknown senders.

CYBER SECURITY TALES: EQUIFAX (2017)

Adapted from Federal Bureau of Investigation press release, Federal Trade Commission statement, CSO Online article, and United States Attorney's Office press release.

Equifax is a company that provides access to personal credit scores. Credit scores provides financial lenders with information about whether or not someone is good at paying back money that they borrow. In 2017, hackers from China found a weak spot in Equifax's website for dispute resolution. Using this vulnerability as a starting point, the hackers were able to gain access to Equifax's networks and databases. Once inside, they stole personal details from 145 million Equifax customers including their names, addresses, birthdays, and even social security numbers.

Equifax knew of the breach for over a month before they asked the U.S. government to step in. Equifax executives used that time to sell their company stock, which led to accusations of insider trading. Insider trading occurs when someone uses knowledge the public does not have access to to enrich themselves by buying or selling stock on the stock market before anyone else can. U.S. Attorney General William Barr and his team of investigators figured out who the hackers were and took legal action against them.

Attorney General Barr said these hackers were working as part of a bigger plan by the Chinese government. They wanted to take information from Americans to improve their artificial intelligence models they use in computers and robots. They also wanted to know more about U.S. government officials and intelligence operatives.

After being sued by their clients, Equifax agreed to a $425 million settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and all 50 U.S. states and territories on behalf of those affected. The funds were used to take care of affected Equifax customers by replacing stolen money, time spent by consumers to resolve these issues themselves, paying legal fees, and any other issue associated with identity theft. Identity theft is a crime when someone secretly takes your personal information, like your name and social security number, and uses it to pretend to be you to buy things or get money in your name.

This Equifax data breach teaches an important lesson: it is important for companies to keep their customers' personal information safe online. Big companies and governments need to work hard to protect our information from hackers. That way, our private information stays private.

CYBER SECURITY TALES: MARRIOTT (2018)

Adapted from Federal Trade Commission press release "The Marriott Data Breach"

In 2018, hackers targeted the Marriott International hotel chain by breaking into Marriott's Starwood reservation system. This is where the hotel keeps information about the people who stay there. The hackers got into this system and accessed the personal information of up to 500 million people. They saw things like names, where people live, phone numbers, emails, passport details, and credit card numbers.

Marriott discovered that hackers had encrypted information and tried to remove it from their system. Marriott had to figure out how to decrypt the hackers' work to discover what they had attempted to steal. They set up a special website and a phone line where people could ask questions and get help. They also offered a free service for a year that monitored signs of identity theft.

Marriott also told people to check their credit reports and bank statements. A credit report is like a report card that shows how someone uses their money. Looking at a credit report or bank statement helps to see if there's anything strange, like money being used without permission. Marriott suggested that their customers put a fraud alert or a credit freeze on accounts, which is like putting an extra strong lock on sensitive personal information.

Marriott warned their clients about scammers, too. After the breach, scammers could send fake emails pretending they were from Marriott. They could make the breach worse by asking for personal information from clients. However, Marriott said they will not send emails asking for personal information.

This data breach demonstrates that it is really important for companies to keep our personal information safe. Everyone should always monitor their personal information and be on the lookout for anything unusual. It is like being a detective for your own information. You want to make sure everything is safe and sound.

CYBER SECURITY TALES: CAPITAL ONE (2019)

Adapted from Capital One publication "2019 Capital One Cyber Incident | What Happened" and the Capital One website "

In 2019, Capital One, a credit card company, was hacked and private information for about 100 million people in the United States was accessed. The information that was accessed included details like customer names, where they live, and sometimes even more private things like Social Security numbers and bank account details. Social Security numbers are important in the U.S. because they are unique to each person and are often used for larger purchases such as a car or a house. Criminals can use Social Security numbers to commit identity theft. Having a social security number makes it easier for a hacker to claim to be someone they are not.

When Capital One found out about this problem, they acted quickly to stop it. They worked with the FBI, and they caught and punished the hacker who accessed the information under the Computer Fraud and Abuse Act, an anti-hacking law. Capital One thinks they got all the information back and that the person did not use that information to commit any further crimes.

To make sure that something like this does not happen again, Capital One has been working hard to make their systems more secure. This means they are putting in new and better ways to protect the information that people trust them with. Capital One executive Richard Fairbanks said he was sorry that the breach happened, and he wants to make things better for everyone who was affected.

Capital One was sued by several of the customers affected by this breach in a class action suit. They made an agreement in court to help the people who were impacted by this issue with a $190 million settlement.

This data breach shows that keeping personal information safe is really important. It is a reminder that big companies, like Capital One, must keep customer information secure. They need to be watchful and to continue improving their security.

CYBER SECURITY TALES: FACEBOOK (2019)

Adapted from Federal Trade Commission press release "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook"

In 2019, Facebook was punished for not keeping personal information people stored on Facebook private. They were supposed to protect the posts people put on Facebook and keep them private between users and their friends. Instead, Facebook allowed other businesses to buy and access the private information of their users without asking them. Users did not expect Facebook to share their information without asking first.

The Federal Trade Commission (FTC) charged Facebook a fine of $5 billion. That's the most money any company has had to pay for not protecting people's private information.

Additionally, the FTC also told Facebook they had to change how they handle people's privacy by ensuring that all private information is carefully guarded and not shared without permission.

The FTC decision shows that even huge companies like Facebook need to be extra careful with the information people share with them. It is a big reminder that keeping our personal information safe on the internet is super important. Companies like Facebook have a responsibility to make sure they protect the personal information of their users.