India Henry

CYSE 201 - 7:25

21 February 2024

Can you spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake?

One of the main ways people and companies get hacked is through phishing attempts. Phishing attempts are composed of a fake email asking for the user to enter their personal information for a, usually, trusted website or app. In this case, both the email and the website are fake and intended to look as real as possible so users will enter their information which will be stolen and exploited. This can lead to more wide-scale consequences once the hackers start using the information where more people can be put at risk from just one access point. For example, the T-Mobile data breach in 2022 which caused a major financial burden for the company but also thousands of customers' information was put at risk. There are multiple ways hackers can go about gaining access to lots of peoples' information, two ways would be using a phishing attempt against someone with admin capabilities or getting lower level access then giving the low level access admin capabilities. Most fake websites are made to look like real websites, some ways to check if a website is fake or not is to check if the site is secured, https with the padlock symbol to the left. Sometimes the domain name is slightly different from what it is actually supposed to be, domain names can't be the exact same so sometimes the domain is misspelled or off by a letter to make it look as real as possible. Lots of spelling errors is another way to identify if a website is fake, while trusted companies are run by people, so there will be flaws, fake websites can have many errors because they don't go through nearly as many background checks as real websites.

References

Drapkin, A. (2022, August 31). *Data Breaches That Have Happened in 2024 So Far - Updated List*. Tech.co. Retrieved February 20, 2024, from https://tech.co/news/data-breaches-updated-list