I am looking into the “I Love You” cyber attack. This grabs my attention because in my opinion it would be one of the easier cyber attacks to prevent because essentially, the user, the one being attacked, is the one who does the damage to their system by clicking on a sketchy email. I have a pretty good eye for scams on emails, and most of them I wont even open the email if I know that I should not be getting an email about a certain website, subscription or service because I have never used that service before. I also look at the email address who sent the email which can be a good tell. at5jg5hktuh@net.cy.qyehet2.com should not be sending you emails about your Netflix subscription.

This attack was significant because of how many people and devices it infected. Forty-five million computers had the virus in just ten days. Twenty years later and it still stands as an infamous attack. The attackers exploited human trust that maybe someone did actually send them a love letter. They exploited curiosity, “Do I have a secret admirer?". To a point you could argue that outdated software had a play. A lot of email inboxes now would not allow an email like this to make it to the main inbox page and instead would send it to the spam folder. However there are still plenty of spam and virus bearing emails that can make it to your main inbox waiting for you to click on them.

Over 20 years ago I am sure those filters on email inboxes were sub par at best and while some may have blocked that email, others it went right through all security measures. The computers were immediately infected with the virus which shared vulnerable data with the hacker. The individuals being hacked were probably a lot more careful about what emails they opened after learning of the attack. That is a positive takeaway. Hopefully those forty-five million people are more educated on cyber safety when it comes to emails.

Making the social media post below really made me think about the positives and negatives of an online presence. If this “I Love You” attack happened today most people would know about it within minutes because of social media posts like I made below. This is a great thing. Twenty years ago communication was not that fast or instantaneous. The negatives might outweigh that though. Having a large online social media presence just opens you up to more possible attacks and gives the public way more information on you than they would have been able to find twenty years ago. Hacking into someone's social media can and will be the start of stealing someone's identity. This is not part of the assignment but all wraps back to how safe you are with your cybersecurity. Let social media be the way you receive news to help keep you safe and don’t let it be a vulnerable place for attackers to build a profile on you and steal your data and or your identity.


WEBINAR
Prevent Data Breach
1 September 2025
09:00 - 11:00 AM
JOIN US
There has been phising emails sent to over 2,000 campus students that can put a virus on your device. DO NOT click on these emails and always invesitgate any incoming emails. Learn more on how to keep your system safe at this webinar.
Let's talk about this with Data Security Expert in this webinar!
Speaker
Chiaki Sato
Data Security Expert
Host
Neil Tran
Analyst
Registration
cybersecurity.com
Are you interested to join us?
YES
YES