Security Breach

Emily Harrison

What is a Security Breach?

- A Security Breach is when someone gains unauthorized access to a network, service, or device.
- Not to be confused with a Data Breach which is usually when the security breach has occured and any time of data or personal information has been taken.

Different types of Security Breaches

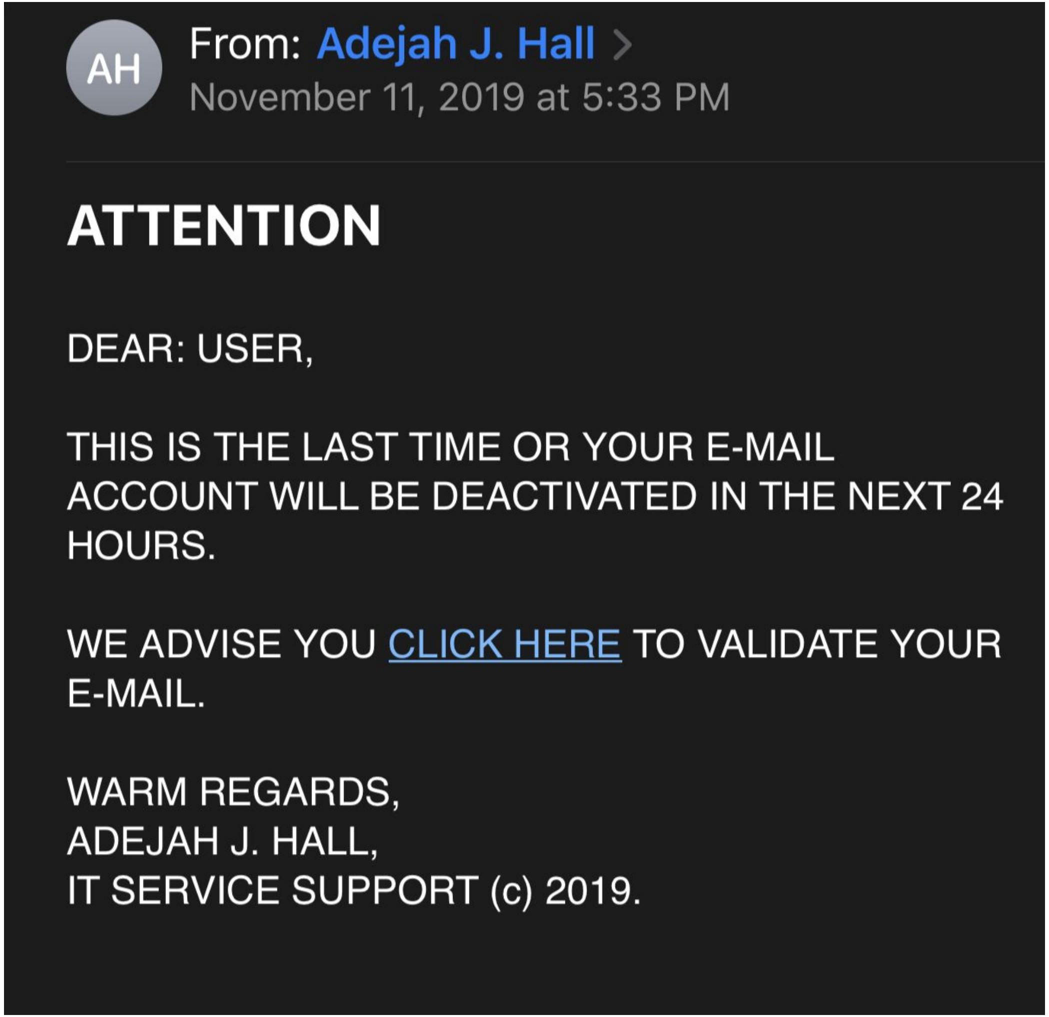
1. Viruses, spyware, and other malware
    - Some of the most common ways for this type of security breach to occur is through email containing the virus.
    - It is also common in downloads or even websites.

2.Impersonation of an organization

Sometime CyberCriminals will create a email or website that looks like it could be and organization or company.

When a email is targeted at one person this is called phishing.

This tactic is known as phishing — or spearfishing, if the email is highly targeted to a specific person.



From: Adejah J. Hall >
November 11, 2019 at 5:33 PM

ATTENTION

DEAR: USER,

THIS IS THE LAST TIME OR YOUR E-MAIL ACCOUNT WILL BE DEACTIVATED IN THE NEXT 24 HOURS.

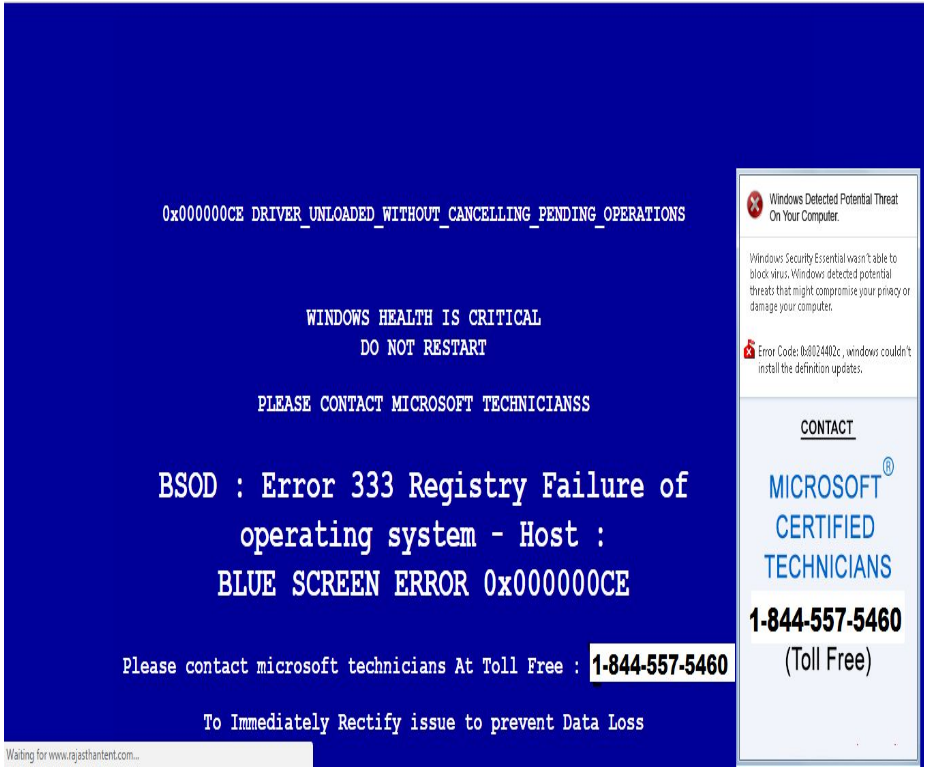
WE ADVISE YOU CLICK HERE TO VALIDATE YOUR E-MAIL.

WARM REGARDS,
ADEJAH J. HALL,
IT SERVICE SUPPORT (c) 2019.

For example, not to long ago a email was sent out through CSU asking for students to change their usernames and passwords by clicking a link that was provided.

3.Denial of service (DDoS) attacks

A denial-of-service attack is capable of crashing websites. Hackers can make a website — or a computer — unavailable by flooding it with traffic making it inaccessible . DDoS attacks are considered security breaches because they can overwhelm an organization’s security devices and its ability to do business. DDoS attacks often target government or financial websites .



0x000000CE DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS

WINDOWS HEALTH IS CRITICAL
DO NOT RESTART

PLEASE CONTACT MICROSOFT TECHNICIANSS

BSOD : Error 333 Registry Failure of operating system - Host :
BLUE SCREEN ERROR 0x000000CE

Please contact microsoft technicians At Toll Free : 1-844-557-5460

To Immediately Rectify issue to prevent Data Loss

Waiting for www.rajasthantent.com...

Windows Detected Potential Threat On Your Computer.

Windows Security Essential wasn’t able to block virus. Windows detected potential threats that might compromise your privacy or damage your computer.

Error Code: 0x8024402c , windows couldn’t install the definition updates.

CONTACT

MICROSOFT® CERTIFIED TECHNICIANS

1-844-557-5460
(Toll Free)

4.Cybercriminals can also exploit software bugs or upload encryption software onto a network to initiate ransomware attacks — in essence, demanding a ransom in exchange for the encryption key. Or intrusions may occur inside an organization, with employees seeking to access or steal information for financial gain.

Target Security Breach

Sources close to the investigation said the attackers gained access to Target's network on Nov. 15, 2013 with a username and password stolen from Fazio Mechanical Services, a company that specializes in providing refrigeration and HVAC systems for companies like Target.

How did the company have access to the information?

- Fazio apparently had access rights to Target's network for carrying out tasks like remotely monitoring energy consumption and temperatures at various stores.
- The hackers first tested the data-stealing malware on a small number of cash registers and then, after determining that the software worked, uploaded it to a majority of Target's POS systems.
- Between Nov. 27 and Dec. 15, 2013, the attackers used the malware to steal data on about 40 million debit and credit cards. U.S., Brazil and Russia.

How this could have been prevented.

- This security breach could have easily been prevented if Fazio were not given access to Target’s network that held all of their information.
- If the username and password had to be changed every few weeks it could have prevented the breach.
- Limit the number of people that have access to sensitive information.
- Create Different Networks for different data/information