unext

Download Now

THE UNEXT INSIDER

★★★★★★★ BREACH HIGH

10 BILLION PASSWORDS
stolen in the biggest data breach ever

200 MILLION
users affected as 9.4GB X data leaks

1.4GB of NSA
data leaked, exposing classified data

In the book This Is How They Tell Me The World Ends, investigative journalist and author Nicole Perlroth describes hackers as ones who enjoy the intellectual challenge of creatively overcoming or circumventing limitations.

The book also talks about how cyberwarfare, cyberespionage, and instances of security breaches have been increasing in ways trivial and unimaginable.

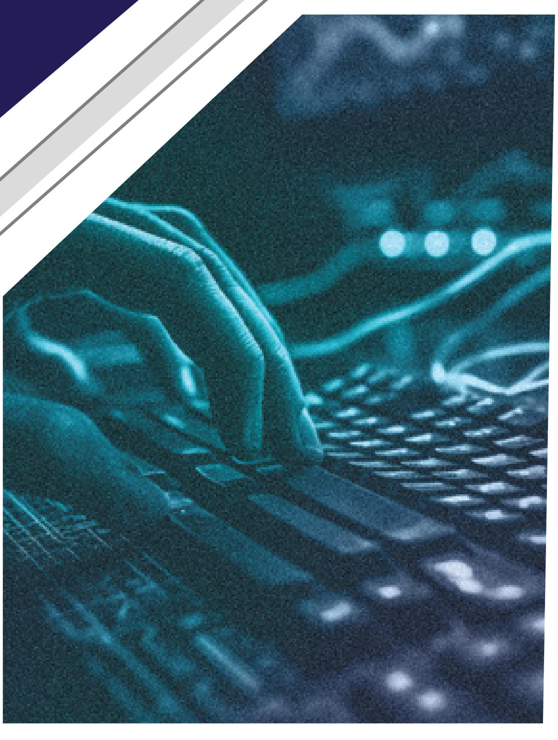
So, if you've always felt assured that your enterprise has been cyber vigilant, here are some of the naivest ways to get data hacked.

Password Guessing – Company@123?

Hackers play Family Feud with servers by developing programs capable of running thousands of password combinations. These are mostly the default password preferences or alphanumerical combinations strategically customized to meet the preferences of a target such as the pet name, phone number, date of birth and similar.

With a brute-force attack, they can unlock systems and servers in less than a few minutes.

Keystroke Entries Recording



During the World War, Russians intercepted American messages by recording keystrokes of their typewriters, in real-time. This breakthrough strategy is now used in digital devices as well.

Through a malware called keyloggers, hackers can record what you type on your computer including every single password, giving them free-flowing access into systems and servers.

This is alarming for enterprises, specifically, finance teams, where keystrokes to enter company credit/debit card details can be recorded and used later to extract funds.

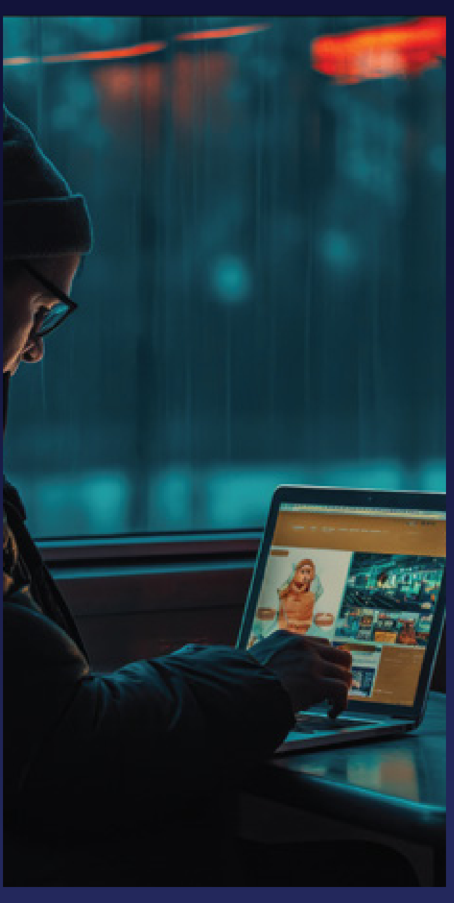
Download our case study on the Java-specific Application Security Program we implemented for a prominent enterprise. **Download Now**

MITM Attacks

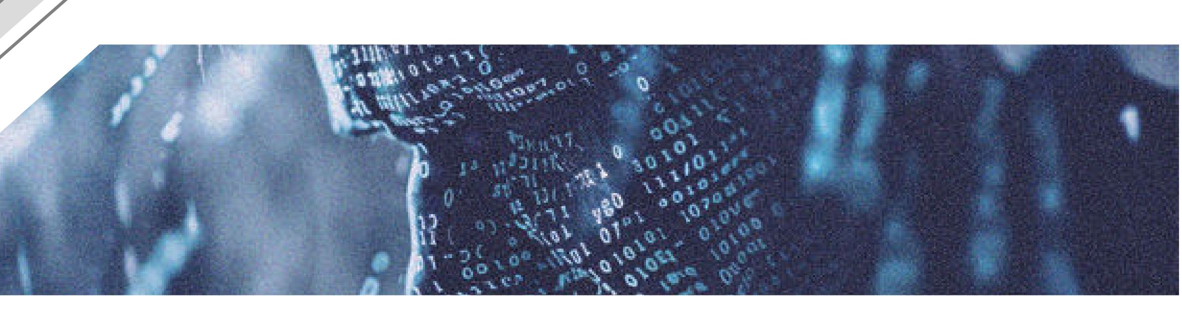
Abbreviated as Man In The Middle Attacks, this is perhaps the most deceptive and prominent ways hackers gain access to sensitive data and information.

By setting up hotspots that are very much authentic, hackers gain instant access to your employees' digital footprints. This gives attackers the ability to secretly intercept, observe, and relay information enroute.

If sights like employees working out of cafes, metros, cabs, and other public places are common in your vicinity, be assured that the chances of hacking their systems are simple.



Juice Jacking



Working out of airports and hotels is fancy but they pose their own risks. Juice jacking is a simple technique of deploying a compromised USB charging port to transfer malware. Devices that then plugin to such ports for charging are hacked to steal data, monitor activity, or even take full control.

Surprised? We barely scratched the surface.

With each passing day, hackers are coming up with surprising ways to exploit vulnerabilities. The only strategy to mitigate attacks is by having a resilient workforce.

Through focused L&D initiatives and training programs deployed by trusted talent transformation partners like UNext, you can nurture cyber-awareness at a cultural level in your organization.

Our bespoke programs for different hierarchies in your enterprise ensure holistic safeguarding of assets and resources. We urge you to revisit your cybersecurity quotient and fill skill gaps with our learning interventions.

To nurture a cyber-resilient workforce, explore our programs today. **Connect Now**

Email: corporate.solutions@u-next.com | Phone: +91 90198 87000