

Forum:[Hack Forums](#)

Thread: [\[CYBERSEC SERIES #10/10 \] Lessons From The Biggest Cyber Attacks in History](#)

Mastercarder - June 7, 2026, 3:04 pm

INTRODUCTION

Cybersecurity is often learned through failure.

Some of the most important lessons in security didn't come from textbooks, certifications, or classrooms.

They came from real-world incidents where organizations lost millions of dollars, exposed sensitive information, disrupted critical infrastructure, and permanently damaged their reputations.

Every major breach leaves behind lessons.

The organizations involved pay the price.

Everyone else gets the opportunity to learn from it.

In this final installment of the CyberSec Series, we'll examine several of the biggest cyber attacks in history, what caused them, and what lessons still apply today.

CASE STUDY #1 — EQUIFAX

What Happened?

In 2017, Equifax suffered one of the largest data breaches in history, exposing the personal information of approximately 147 million people.

Lesson Learned

A known vulnerability can be just as dangerous as a zero-day when organizations fail to patch systems promptly.

How To Protect Yourself

? Keep systems updated

? Monitor security advisories

? Prioritize critical patches

CASE STUDY #2 — MT. GOX

What Happened?

Mt. Gox was once the largest Bitcoin exchange in the world before collapsing after losing hundreds of thousands of Bitcoins.

Lesson Learned

Centralized platforms can become dangerous single points of failure.

How To Protect Yourself

- ? Diversify storage
- ? Use secure backups
- ? Never keep everything in one place

CASE STUDY #3 — COLONIAL PIPELINE

What Happened?

A ransomware attack disrupted fuel distribution operations across parts of the United States and demonstrated how cyber incidents can impact real-world infrastructure.

Lesson Learned

One compromised credential can create massive consequences.

How To Protect Yourself

- ? Enable MFA
- ? Use unique passwords
- ? Monitor account activity
- ? Remove unused accounts

CASE STUDY #4 — WANNACRY

What Happened?

WannaCry spread globally and affected hospitals, businesses, and government organizations across more than 150 countries.

Victims lost access to systems and data due to ransomware encryption.

Lesson Learned

Outdated systems become liabilities.

How To Protect Yourself

- ? Keep operating systems updated
- ? Maintain backups
- ? Remove unsupported software
- ? Test recovery procedures

CASE STUDY #5 — SONY PICTURES

What Happened?

Sony Pictures suffered a major breach that exposed emails, employee information, internal documents, and unreleased content.

Lesson Learned

Sensitive information should be protected before a breach occurs.

How To Protect Yourself

- ? Encrypt sensitive information
- ? Apply least-privilege access
- ? Review permissions regularly
- ? Separate critical systems

5 LESSONS EVERY MAJOR BREACH TEACHES US

- ? Patch Your Systems
- ? Use Strong Authentication
- ? Back Up Important Data
- ? Limit Access
- ? Prepare Before An Incident Happens

FINAL THOUGHTS

The biggest cyber attacks in history are more than headlines.

They are lessons.

Equifax taught us the cost of poor patch management.

Mt. Gox demonstrated the dangers of centralization.

Colonial Pipeline highlighted the risks of compromised credentials.

WannaCry showed the consequences of outdated systems.

Sony Pictures proved how damaging data leaks can become.

Different incidents.

Different targets.

The same core lessons.

Technology changes.

Attack methods evolve.

But the mistakes rarely do.

PREVIOUS PARTS IN THIS SERIES

? [Part #1 – You're Probably Easier To Hack Than You Think](#)

? [Part #2 – How People Get Hacked Without Downloading Anything](#)

? [Part #3 – Why 2FA Alone Won't Save You](#)

? [Part #4 – Your Phone Knows More About You Than Your Friends Do](#)

? [Part #5 – What Is A Zero-Day Exploit?](#)

? [Part #6 – DNS Explained: What Happens When You Visit A Website](#)

? [Part #7 – SQL Injection Explained: How Websites Get Exploited](#)

? [Part #8 – Blockchain OSINT: Investigating Cryptocurrency Wallet Activity](#)

? [Part #9 – Password Cracking Explained: Hashes, Salts & Brute Force](#)

? CYBERSEC SERIES COMPLETE (1–10) ?

Thank you to everyone who followed the series from beginning to end.

Stay curious.

Stay cautious.

Stay secure.

Pr0m3th3us - June 17, 2026, 5:14 am

Crazy that 2 out of the 5 were from a country most consider a 3rd world. And in a way it is, people eating grass, bugs and birds just to survive.

Meanwhile in Pyongyang sits some of the best (or worst)? cyber criminals. They made one of the worlds most devastating hacks to this day. Which makes you wonder what will they do next that is bigger then wanacry was....

On a side note...i got about \$11.37 from that equifax settlement....fuckin pricks.

Mastercarder - June 17, 2026, 2:35 pm

(Jun 17, 2026 05:14 AM)Pr0m3th3us Wrote: [\[CITE\]](#) Crazy that 2 out of the 5 were from a country most consider a 3rd world. And in a way it is, people eating grass, bugs and birds just to survive.

Meanwhile in Pyongyang sits some of the best (or worst)? cyber criminals. They made one of the worlds most devastating hacks to this day. Which makes you wonder what will they do next that is bigger then wanacry was....

On a side note...i got about \$11.37 from that equifax settlement....fuckin pricks.

Lol yep. It's always the people you least expect I guess.

Thanks for your response bro.