



22
Dec

Cyber Security Awareness

The 20 Best Movies and TV Shows About Hackers and Cyber Security

For nearly a half-century, cyber security, cyber attacks, and the criminals who perpetrate those acts have been a topic of fascination in Hollywood. With increased tech reliance and adoption beginning at the turn of the 21st century, the appetite for and popularity of these types of movies and TV shows has exploded worldwide.

This collection of titles is perfect for anyone looking to delve into the cinematic world of information security or enjoy an exciting bit of escapism. Every movie and TV show on this list either explicitly centers around cyber security, contains more than a few scenes focusing on the subject, or embodies the spirit of why protecting sensitive data is of the utmost importance.

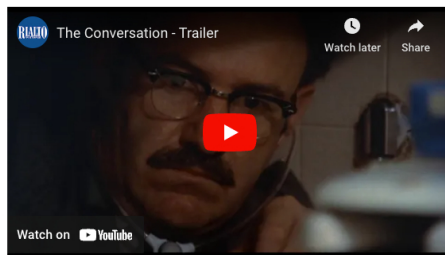
The similarities between the characters and scenarios depicted in these stories, often drawn from real-world events, may surprise you.

What may also surprise you is that, for several of these movies, there are things that we can all learn from them that can apply to our daily lives as cyber security professionals.

We've added some takeaways along with helpful resources for you to several of these amazing movies. Read on to discover where fiction meets reality in the world of cyber security.

1. The Conversation (1974)

Gene Hackman plays a surveillance expert who gets in over his head when a routine job spying on a couple quickly spirals into something far more dangerous. Widely considered Francis Ford Coppola's best non-*Godfather* film, it's a taut exploration of how a lack of data (or physical office) security can hold lives in the balance.



What we can learn from this movie

Something that we, as cyber security pros, can often overlook is physical security. The ability to access restricted areas like data centers allows hackers to get what they're looking for right at the source.

One recent survey shows that up to 74% of executives believe that they're not doing enough to clamp down on physical security incidents. That's an ominous number.

How you can be prepared

Increasing your physical security protocols is just step one in your defense against these kinds of attacks. Awareness is key, and it pays to make sure your employees know how to defend against these malicious individuals.

More resources

Learn about [tailgating](#) (physical) attacks here.

Learn how to detect common social engineering tactics in [this white paper](#).

2. Tron (1982)

In one of the earliest movies centering around hacking, a computer engineer is transported to a virtual world after learning an executive has plagiarized his work. Once there, he's forced to compete in increasingly war-like games, with his only hope for escape is - wait for it - a security program! A sequel, *Tron: Legacy*, was released in 2010.

Search

Categories

Compliance and Governance (9)

Cyber Security Awareness (298)

Data Privacy Awareness (57)

Events (11)

GDPR (9)

News (25)

Phishing (91)

Recent Posts

What is Baiting in Cyber Security?

7 Smishing Examples and How to Protect Yourself

What is Swatting? What to Look for and How to Defend Yourself

The 2023 Gone Phishing Tournament Results: Everything You Need to Know

Protect your loved ones from phishing, social engineering and other cyber attacks

Tags

- byod
- CISO
- communication tools
- COVID-19 Scams
- credential stuffing attacks
- Cyber security Awareness
- cyber security professional
- Data breaches
- Data Privacy
- End user engagement
- gartner magic quadrant
- GDPR Training
- governance
- Human Risk
- Information security awareness
- Information security program
- lise lapointe
- malware
- National Cyber Security Awareness Month
- NCSAM
- Password
- phishing
- Phishing scams
- phishing simulation
- ransomware
- Remote working
- Security Awareness Framework
- Security Awareness Training
- social engineering
- Social Networks
- Work from home



What we can learn from this movie

Without getting too existential about it, one thing we can easily take away from this movie is that anyone can target your systems. Insider threats are all too common, and it's the wise network admin who puts the organization first.

How you can be prepared

There are several steps to preparedness against insider attacks, but first is strong internal network and systems permissions for the entire staff. If someone doesn't need access, they don't get it. It's as simple as that. See the below to learn more.

More resources

Discover the steps to identifying and preventing insider threats in your organization [here](#).

3. WarGames (1983)

A pre-Ferris Bueller Matthew Broderick plays David, a high school-aged computer whiz who accidentally accesses a military supercomputer programmed to simulate ... well, precisely what the title suggests. This film was one of the first smash hits with a hacker as the central character, grossing \$125 million worldwide against a \$12 million budget.



What we can learn from this movie

The computer in WarGames makes a simple request: "Would you like to play a game?" Well who wouldn't like to play a game? Unfortunately, the results of playing the game—at least in this movie—nearly set off a global nuclear war.

While the stakes may not be as high at your business, it may feel like they are if someone were to answer the wrong question from a clever phishing email.

How you can be prepared

Do your employees know what to do when they receive an email that could be a phishing attack? Phishing simulation is one of the ways that you can make sure that your staff are aware of the kinds of clever, manipulative, and attractive ways that hackers try to gain access to your systems.

Let's face it, cyber security ain't no game, and your organization needs to be able to assess your employees' level of awareness on a regular basis.

More resources

Get the Gamification for Cyber Security Awareness Training Success white paper [here](#).

4. Sneakers (1992)

Robert Redford stars as Martin Bishop, the head of a security specialists team that performs ethical hacking for large organizations. However, Bishop's got a few skeletons in his closet, and when NSA officers task him with retrieving a black box item in exchange for a clean slate, it's an offer he can't pass up. Initially conceived by Lawrence Lasker and Walter Parkes, the writing duo behind WarGames.



What we can learn from this movie

Oh boy. There are so many takeaways to be gleaned from Sneakers, but let's focus on what made the team in this movie so effective: Diversity.

Each member of the Sneakers team had a specific set of skills... skills that make them a nightmare for people like the ones in the movie (to paraphrase Liam Neeson in Taken).

Where one person may not have found the answers by themselves, having a team of people from different backgrounds with different experiences and expertise is what keeps this team together.

How you can be prepared

Diversity, Equity, and Inclusion (DEI) are a lot more than just buzzwords. Study after study shows how DEI can improve the workplace in many different ways.

As an example, [this study](#) by Hult International Business School states that "Diversity... has been shown to improve retention and reduce the costs associated with employee turnover." The [Harvard Business Review](#) tells us that companies with greater diversity are 70% more likely to capture more markets.

We could go on, but suffice it to say that teamwork makes the dream work when you can approach problems from a lot of different angles.

More resources

Learn about creating an inclusive work environment in [this post](#) on the [Terranova Security blog](#).

5. Ghost in the Shell (1995)

Based on a manga of the same name by Masamune Shirow, this neo-noir animated thriller has become one of the most influential cyberpunk entertainments in popular culture. Highlights include a plot centered around the hunt for a hacker known as the Puppet Master and philosophical questions about an individual's role in a hyper-tech-reliant world.



6. Hackers (1995)

Arguably the most 90s pick on this list, *Hackers* is an energetic romp of a thriller pitting a band of school-aged hackers against a corporate extortionist seeking a big payday. It's also a stark reminder of how new and foreign the internet felt to the average consumer in 1995, with scenes echoing [The Hacker Manifesto](#), an essay published nearly a decade earlier.



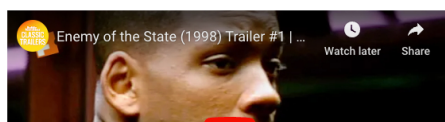
7. The Net (1995)

Sandra Bullock stars as a systems analyst who works remotely in California and becomes embroiled in a deadly conspiracy after receiving a mysterious floppy disk that backdoors into a well-known computer system. The plot includes numerous cyber security topics, including identity theft, spoofing, and early examples of cyber terrorism.



8. Enemy of the State (1998)

Before real-life leaked documents (paging Edward Snowden) revealed the shocking extent of computerized surveillance, *Enemy of the State* posits how devastating this unprecedented and unchecked access to consumer data can be. Unsurprisingly, then-NSA Director Gen. Michael Hayden was "appalled" at the film's depiction of the agency.





9. Office Space (1999)

A work-life satire that takes place at a late-90s software company, *Office Space* earns a place on this list due mainly to the caper at its center. Three disgruntled employees decide to get a little revenge against their corporate overlords by infecting the accounting system with a virus and making off with hundreds of thousands of dollars. Proof positive that technological safeguards can't guarantee information security.



What we can learn from this movie

Apart from the fact that if you're going to offer someone cake, you should make sure that the person actually gets some cake, and to echo the sentiment above, this movie shows us that no matter how many technical safeguards you may have in place, information security is not a foregone conclusion.

As scary as that may sound, the solution may be as simple as making sure that your employees are as happy as Milton with a red stapler.

How you can be prepared

According to Forrester, 66% of people who work in cyber security have symptoms of extreme stress or burnout, while 51% of those have sought out medication for their mental health. How can you help? [This post](#) on the Terranova Security blog lists five ways you can help your employees avoid burnout:

- > Use security automation to support your human analysts
- > Outsource some security tasks
- > Create a comprehensive security plan
- > Don't have unrealistic expectations for your staff
- > Ease the workload with cyber security awareness

Overall, making sure that your entire company is trained in cyber security best practices helps your IT team to feel more supported, more optimistic, and less stressed.

More resources

Check out this blog post on the Terranova Security blog: [Cyber Security Burnout: What it is and 5 Actionable Tips to Avoid It](#)

This white paper will help you make sure your entire team is helping to avoid cyber security burnout: [From Data Protection to Cyber Culture](#)

10. The Matrix (1999)

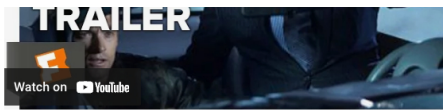
No list of fictional movies or TV shows that touch the topic of cyber security is complete with *The Matrix*. It's a well-known pop culture touchstone that continues to influence and inspire tech odysseys in art. The film's themes have only become more relatable with time, especially with advances in VR technology pushing us closer to the reality depicted in this classic.



11. Swordfish (2001)

A notorious hacker (Hugh Jackman) is coerced into cracking a secure Defense Department server. After the attack is successful, he's asked to program a multi-headed worm for individuals purporting to be government agents, though nothing is as it seems. Come for the manic techno thrills. Stay for the wacky editing and even wackier John Travolta facial hair.





Without adding any spoilers in case you have somehow never seen *Swordfish*, the real antagonist in this movie is the worm programmed by Hugh Jackman's character while John Travolta threatens to make him grow facial hair even worse than his own (not really, but like, come on, John).

A worm is a type of ransomware that lets criminals hold data for ransom. According to [this post](#), trojan worms "have become so sophisticated over the years, that they are virtually impossible to remove without the help of the criminals who designed them."

And once again, the delivery system is almost always something as benign as an email with an attachment that is too attractive for someone to pass up.

How you can be prepared

The first step is to be aware of the many ways that ransomware can affect your systems. Whether it's through phishing, malvertisement, traffic distribution systems, or other means, we are all targets for ransomware. Prevention is as simple as [education](#). An investment in your people that gives them the information they need to recognize the risks along with ongoing education is key to preventing ransomware.

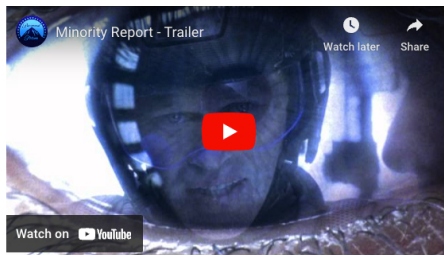
More resources

Learn more about ransomware and how to [prevent it by clicking here](#).

Read this post on the Terranova Security blog: [Three things you can do to protect your workforce against ransomware attacks](#)

12. Minority Report (2002)

If you think current AI and machine learning efficiency is too invasive, what if law enforcement could arrest and incarcerate criminals before committing a crime? It's the intriguing premise of this high-octane Spielberg-Cruise actioner, which asks just as many philosophical questions about technology integration and habit monitoring as it answers.



13. V for Vendetta (2005)

Based on the British graphic novel of the same name, this adaptation updates the narrative to include commentary on government surveillance and media manipulation. However, the iconic Guy Fawkes mask has been the story's lasting contribution to cyber security culture, now an image commonly associated with the hacking network Anonymous.



What we can learn from this movie

Well this is a tough one. Depending upon who you are and your position in the world, the character, V, may be either a good guy, or a bad guy.

I think (and this is where I add the common initialism, IMHO), that one of the most important lessons we, as cyber security professionals, can take away from this movie is the importance of vigilance in maintaining a healthy cyber security culture. Let's explore that a little further.

How you can be prepared

Culture plays an incredibly important role in maintaining a healthy cyber security environment. [This article](#) (which is referenced [here on our blog](#)) by the Tuck School of Business talks about the importance of culture as a cyber security tool:

An organizational culture that values sound security practices is far more effective than regulations that simply mandate them.

The idea is that with ever-present vigilance against threats of any kind, the employees of an organization with a strong commitment to cyber security culture need not resort to wearing Guy Fawkes masks in order to carry out a vendetta of any kind. The message, though, is clear: It's up to you.

More resources

Read [How to Build a Strong Security Awareness Training Program in 2023](#) on our blog.

Read [5 Essential Elements for People-Centric Security Awareness Training](#) on the Terranova Security blog.

14. Live Free or Die Hard (2007)

In the fourth installment in the popular action franchise, Bruce Willis returns as NYPD detective John McClane. His mission: To stop a cyber terrorist targeting government and private sector systems as part of a plot to disable critical pieces of United States infrastructure. Justin Long brings a comedic element as another hacker who acts as McClane's tech-literate sidekick.



15. The Social Network (2010)

One of the most respected movies of the 21st century, David Fincher's exploration into Facebook's origins and rise to prominence is as unsettling as it is darkly funny. The direct link to cyber security involves Facebook's precursor Facemash, which Zuckerberg created by hacking into Harvard databases to obtain photos of female students for the "hot or not" rating site.



16. The Fifth Estate (2013)

Directed by Bill Condon of *Chicago* fame, this film is a fictionalized account of the founding and fallout of WikiLeaks, a website dedicated to leaking classified information while protecting anonymized sources. Though allegedly embellished in terms of historical accuracy, this film showcases how information security (or lack thereof) can be easily manipulated for personal or political gain.



17. Ex Machina (2014)

In early 2015, IGN reviewer Chris Tilly [described](#) this movie as "essential viewing for anyone with even a passing interest in where technology is taking us." With a search engine coder serving as the protagonist and audience proxy, the story asks pointed questions about artificial intelligence, the dangers inherent in its development, and the security issues that may arise when we can no longer distinguish humans from machines.



18. Mr. Robot (2015–2019)

Before his Oscar-winning turn as Freddie Mercury, Rami Malek was primarily known for portraying cyber security engineer and hacker Elliott Alderson on *Mr. Robot*. The show's title refers to the anarchist who recruits Alderson into a hacktivist collective that wants to cancel consumer debt by

encrypting large swaths of corporate data.



19. Snowden (2016)

As with *The Fifth Estate*, a list like this would be incomplete without a mention of the Oliver Stone-directed account of how and why Edward Snowden leaked classified NSA information. However, unlike the WikiLeaks dramatization, Stone actually met with Snowden several times and, for security reasons, supposedly had to write portions of the script on a laptop without internet access.



20. Westworld (2016–2022)

Arguably the most epic and intense entry on this list, HBO's reimagining of the 70s cult classic is an examination of cyber security woes as a vivid sci-fi-western hybrid. Besides the general topic of AI regulation, which has been a recurring theme over several seasons, specific plot points hinge on insider threats, malware, and vulnerabilities inherent in an Internet of Things setup.



Want to learn more about protecting yourself from fraudsters and hackers?

Access the Cyber Security Hub for free.

[ACCESS THE HUB](#)

Share: [f](#) [x](#) [in](#) [t](#)

Newer [← Top 5 Data Security Incidents of 2023 and Predictions for 2024](#) [The Most Important Cyber Security Trends of 2024](#) [→](#) Older

TRAINING

Cyber Security Training for Employees
Privacy Awareness
Click and Launch
Compliance and Governance
GDPR
Phishing Simulation
Cyber Games

FREE TOOLS

Cyber Security Hub
eBook – The Human Fix to Human Risk
Phishing Free Trial
Reports and Guides
Cyber Challenges Demo

STAY CONNECTED

[f](#) [in](#) [t](#) [v](#)

COMPANY

About Terranova Security
Join Our Team

GET IN TOUCH

Contact Us
Customer Support
Cybersafe and Sound Newsletter

SUBSCRIBE TO THE CYBERSAFE AND SOUND NEWSLETTER

Your cyber security awareness newsletter

Business Email*

Email must be formatted correctly.

[SUBMIT](#)

GET STARTED

SIGNING UP FOR NEWSLETTERS INDICATES YOU AGREE WITH OUR PRIVACY POLICY.

[Free Demo](#)

[Request a Quote](#)

[Phishing Simulation Trial](#)

IF YOU DECIDE THAT YOU NO LONGER WANT TO RECEIVE OUR NEWSLETTERS, YOU CAN UNSUBSCRIBE BY CLICKING THE "UNSUBSCRIBE" LINK LOCATED AT THE BOTTOM OF EACH NEWSLETTER.

Copyright © Fortra, LLC and its group of companies. Fortra™, the Fortra™ logos, and other identified marks are proprietary trademarks of Fortra, LLC.
[Privacy Policy](#) | [Cookie Policy](#)



FORTRA
Terranova Security