FORTRA

Cybersecurity Myths Debunked

Cybersecurity Experts From Around The World Share Their Favorite Security Myths.

Introduction

The life of a cybersecurity professional looks a lot like the plot of a Greek mythology action movie. We spend years preparing for an attack by an unknown creature, basing our strategy on tales passed down from cybersecurity warriors before us. DDoS attacks are waged by the mythical Hydra with multiple heads attacking from every angle; phishing emails are released, disguised as alluring calls from beautiful Sirens.

Along with these aggressions come the myths of how best to defend against such attacks. Which is why Fortra set out to debunk some of the most popular cybersecurity myths that exist today.

Meet the Experts

We asked six uniquely-qualified security experts from around the world to debunk their favorite IT security myths.

Read on to discover their answers.

Michael Bruemmer
Vice President
Experian™ Data Breach Resolution
& Consumer Protection

Troy Hunt
Author at Pluralsight
Microsoft Regional Director

Creator of Have I Been Pwned? (HIBP)

Kevin Beaver
Independent Information Security Consultant
Principle Logic, LLC

Author of Hacking For Dummies, The Practical Guide to HIPAA Privacy *and* Security Compliance*, and 10 other security books*

Bob Carver CISM, CISSP, M.S
Sr. Security Analyst
Verizon Wireless

Jonathan Lampe, CISSP, GSNA, CFTP
Executive Director
Certifies File Transfer Professional (CFTP) Program

Ben Cole
Senior Site Editor
SearchCompliance.com, SearchCIO.com

Myth #1

The Majority Of Consumers Are Not Vulnerable To Identity Theft.

"A common misconception I've observed when it comes to IT security is that despite having a large digital footprint, consumers underestimate the risk of their online behaviors resulting in identity theft.

According to a recent Experian study, consumers are generally aware of the threat, but underestimate their personal exposure and actually exhibit online behavior that could harm vs. help their chances of becoming a target.

For instance, 43 percent of respondents use public Wi-Fi to shop online, 33 percent share online accounts' usernames and passwords with others, and 29 percent share mobile device passwords. These are dangerous habits that voluntarily lead personally identifiable information (PII) to become vulnerable to cybercriminals online.

Clearly, there's a disconnect between consumer awareness and understanding, as the majority (62 percent) of respondents said the security of their personal information online was a 'minor concern they worried about sometimes.'

What's more, they're even less concerned about their PII appearing on the dark web. There's a major learning opportunity for consumers to educate themselves on the risks of identity theft and proper online behaviors to protect their personal data online."

Michael Bruemmer
Vice President
Experian® Data Breach Resolution & Consumer Protection

Share this

Myth #2

Meeting Compliance Regulations Is The "Gold Standard" Of Risk Management In Cybersecurity.

"A common misconception is that if a business entity is compliant with a security standard such as NIST or ISO that they have reached the 'gold standard' of risk management in cybersecurity.

This should be considered a valiant good start, but nowhere near the 'gold standard.'

I have seen businesses that have focused primarily on compliance to standards and not on threat intelligence and analytics that did not fare well on discovering compromised endpoints. This could be due lack of visibility or perhaps overconfidence.

On the other end, I have seen entities that focused on threat intelligence and analytics that were able to discover compromises faster and more often than other business with far more controls in place.

The reality is you need to attack from both ends; compliance/controls and threat intelligence with analytics."

Bob Carver CISM, CISSP, M.S.
Sr. Security Analyst
Verizon Wireless

Share this

Myth #3

You Must Change Your Password Every 90 Days.

"The misconception that comes immediately to mind is the one about password rotation, where they say 'every three months you need to change your password.' It's really interesting because we have this mix of opinions at the moment where most organizations say 'you must rotate your password every 90 days in order to keep it secure' and on the other side you have The National Cyber Security Centre of the British government and NIST saying 'don't do this because it makes it worse!'

And I love the rationale that they use, it's just so pragmatic:
If someone gets your password, they're not going to wait 90 days to use it, they're going to use it now!"

Troy Hunt
Author at Pluralsight
Microsoft Regional Director

Share this

Myth #4

Hackers Aren't Interested In Your Supply Chain.

"One of the worst misconceptions in IT security today might be that hackers aren't interested in your supply chain.

Companies I've worked with often make their largest security investments on customer-facing servers, internal workstations, and their workforce, leaving many of the 'back end' supply chain resources to fend for themselves. Often these resources are 'legacy' but nonetheless mission-critical EDI and file transfer technologies with dozens of known vulnerabilities.

Smart hackers are often very interested in these supply-chain deployments for three reasons. First, they know these systems control millions of dollars of payments and shipped goods. Second, they know these systems open doors into core systems such as mainframes and customer databases. And third, they know that systems that communicate with partners are often Internet-exposed.

Fortunately, many of the same principles that protect other IT infrastructure can be applied to supply-chain technology, including patching, use of secure protocols, use of strong credentials, and monitoring. Unfortunately, the question is usually whether the will, budget and know-how to actually implement appropriate security controls in supply-chain environments actually exists."

Jonathan Lampe, CISSP, GSNA, CFTP
Executive Director
Certified File Transfer Professional (CFTP) Program

Share this

Myth #5

Cybersecurity Is An It-Centric Problem.

"Too many people tend to believe that security is an IT-centric problem. Sure, a couple of decades ago, that's how it started out but security has since evolved to a core and critical business function and needs to be treated as such.

Unfortunately, people from every side: IT, management, and users still automatically assume that security is technical in nature and is being properly handled by IT staff. IT professionals perpetuate this by proclaiming that everything is in check when, looking behind the scenes, it's really not.

This false sense of security is a large part of why we are still experiencing incidents and data breaches. Well, that combined with the lawyers who have jumped aboard the security train and are trying to stop the attacks with their paperwork."

Kevin Beaver
Independent Information Security Consultant
Principle Logic, LLC

Share this

Myth #6

The Key To Security Is To Replace Any Human Tasks With Automation.

"My least favorite IT security misconception is that data security can be completely automated. It's well known that humans remain the biggest IT security vulnerability—some of the biggest and most expensive data breaches in the last five years were the direct result of human error.

This had led many companies to turn to tech such as artificial intelligence, machine learning, and robotic process automation to take the human element out of the security equation. But next-generation IT security should focus on ways to integrate these tech advances with human-driven capabilities such as advanced data analytics techniques or intrusion detection tools monitored by personnel.

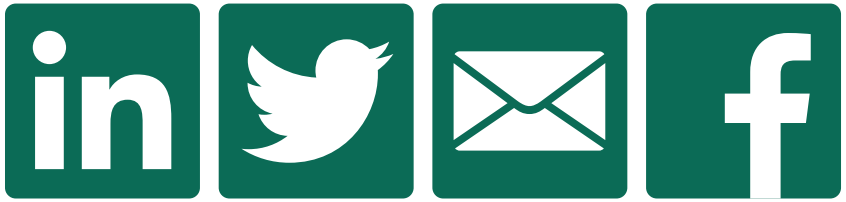
Employees can also still help determine and react to rapidly changing vulnerabilities, a valuable trait as threats and attack vectors continue to change. As a result, the misconception that IT security can be run by 'set it and forget it' type applications is misguided, and potentially dangerous, as threats proliferate."

Ben Cole
Senior Site Editor
SearchCompliance.com, SearchCIO.com

Share this

Do You Have A Favorite Cybersecurity Myth Of Your Own?

Tweet your myth with the hashtag #SecurityMyth to continue the conversation.



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-corp-gd-1022-r1-79d