Lies and Myths in InfoSec

Why are myths and lies even a thing?

INFOSEC IS ALREADY CHALLENGING ENOUGH

Why are myths and lies even a thing?

DAMAGES AND LOSSES ARE OBJECTIVELY HUGE

Why are myths and lies even a thing?

WHY PRETEND THAT THINGS ARE EVEN WORSE?

Why are myths and lies even a thing?

REASON #1: COMFORT

The most dangerous myths and lies are things we're **eager to hear.** This puts us in a **vulnerable state.**

Why are myths and lies even a thing?

REASON #2: FAKE IT 'TIL YOU MAKE IT

- “We just need to close the next round of funding”
- “We just need to hit the growth numbers”
- “We just need to convince them this is critical”

Why are myths and lies even a thing?

REASON #3: BURDEN OF PROOF

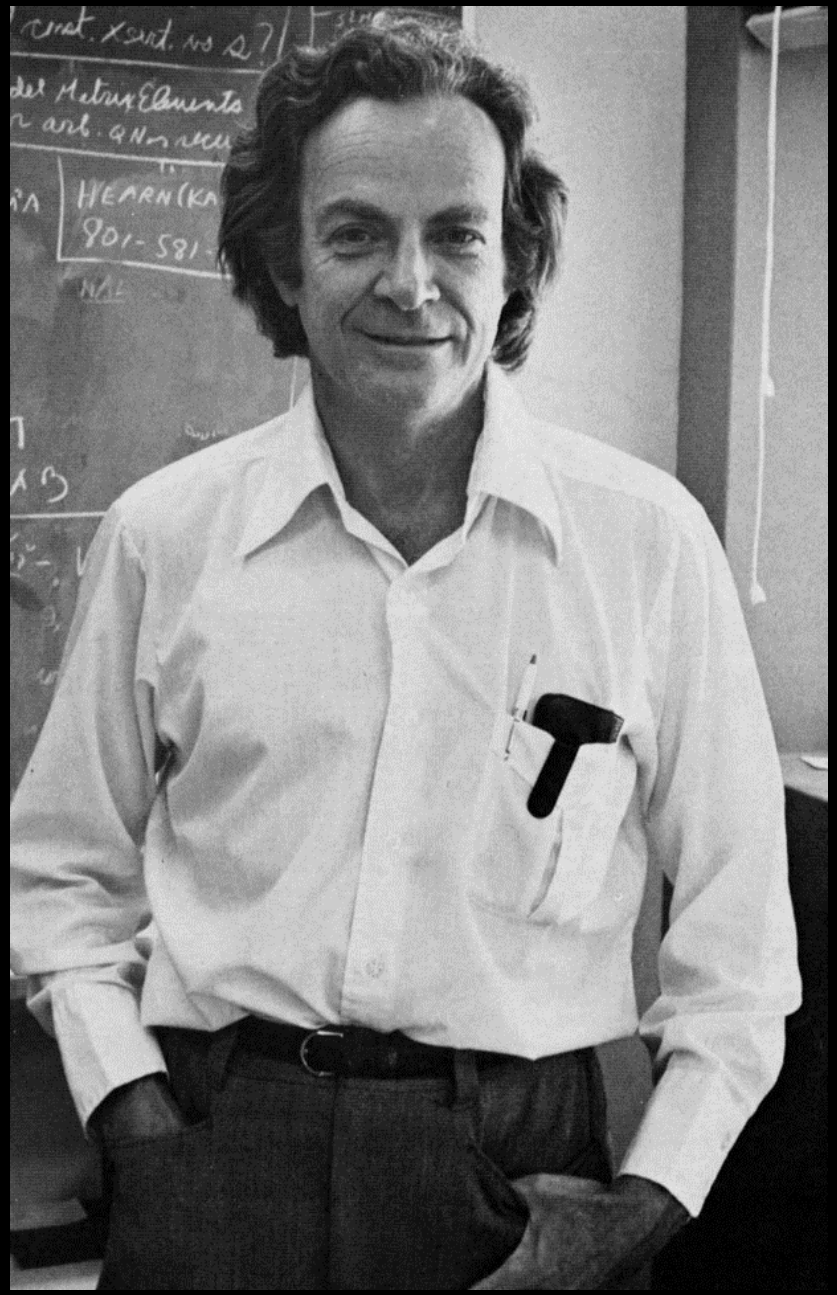
Do I have more energy because of $10 health shakes?

Or because I got 2 more hours of sleep than normal?

2001
CloudNine

2004
CardSystems

2006
Blue Security



Confirmation Bias

”The first principle is that you must not fool yourself - and you are the easiest person to fool."

Richard P. Feynman

Think of your ideas and beliefs as software you're actively trying to find problems with rather than things to be defended.

yourbias.is/confirmation-bias

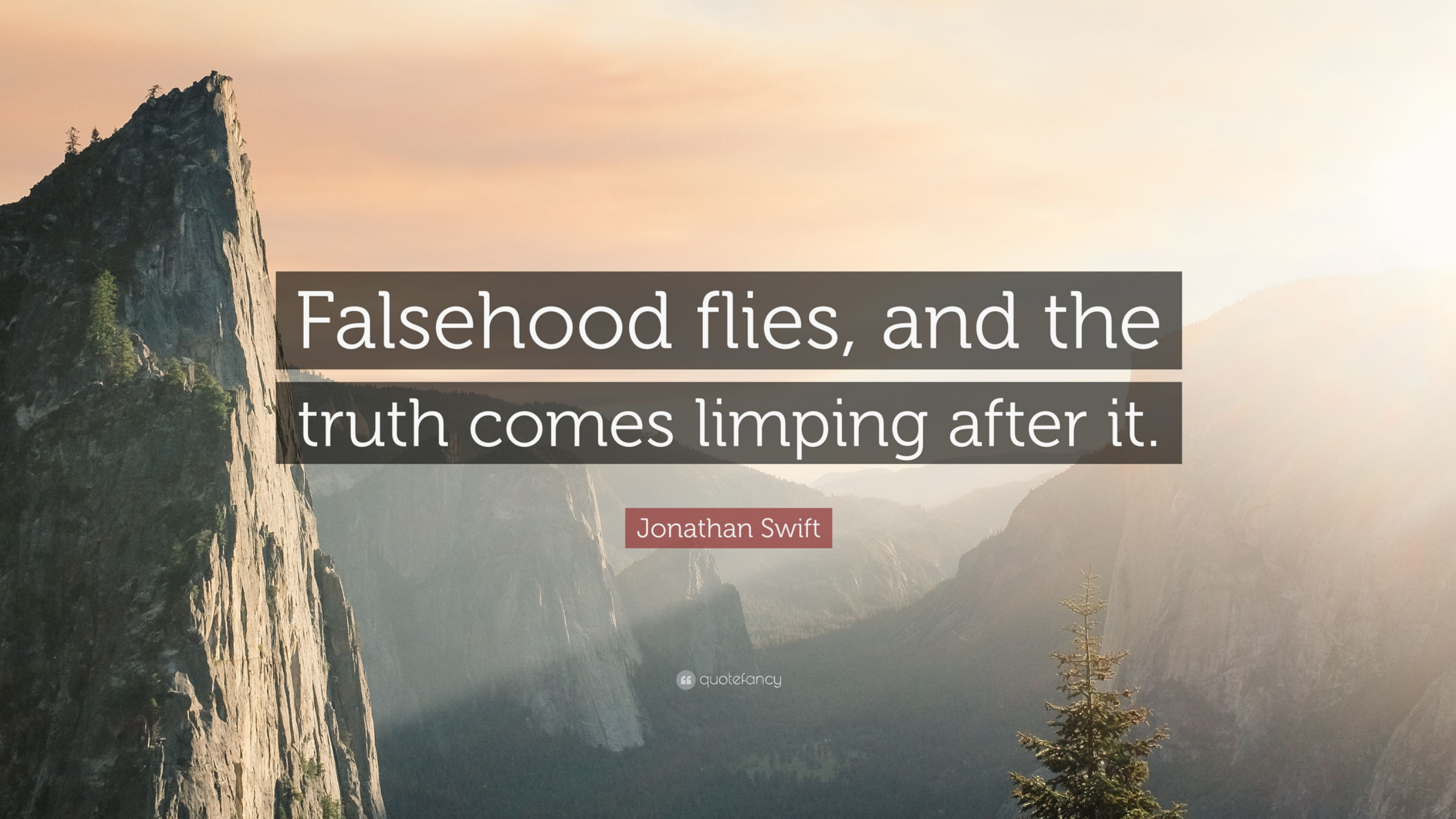
Sunk Cost

How does it feel...

when you find out you've been spreading a myth

for the past 5 years?

yourbias.is/the-sunk-cost-fallacy


Falsehood flies, and the truth comes limping after it.
Jonathan Swift
quotefancy

2001
CloudNine

2004
CardSystems

2006
Blue Security

2007
Verus

2008
Spicy Pickle Restaurants

2011
HBGary Federal

Distribute.IT

DigiNotar

Bad stats hurt the industry's credibility

Bryson Bort @brysonbort · 2h

Oh come on, fine, make up the stats, but at least they should sound vaguely right.

> **SANS Cloud Security** @SANSClo... · 2h
>
> "Cyber crime costs $2.9 billion dollars per MINUTE."
>
> "1.8 million cyber security job shortages."
>
> ...

TO SANS' CREDIT, THEY PULLED THIS DOWN RELATIVELY QUICKLY

But not before hundreds of folks shared it.

Why challenge InfoSec myths and lies?

- **CREDIBILITY**

  Cybersecurity is not a professionalized industry. There are no PE equivalents signing off on blueprints for security programs. If we want to be taken seriously in public forums and private boardrooms, we need to protect our reputation.

- **MISDIRECTED EFFORTS AND RESOURCES**

  Myths and lies can convince us to focus budget and resources on areas that might not be important at all.

- **THE TRUTH TEACHES**

  The truth is invariably more interesting, and the process of getting there almost always teaches valuable, but unexpected lessons.

2001
CloudNine

2004
CardSystems

2006
Blue Security

2007
Verus

2008
Spicy Pickle Restaurants

2011
HBGary Federal

Distribute.IT

DigiNotar

2012
Only Honest

2014
Code Spaces

There's ONE company behind most of the fake stats in InfoSec

“CYBERCRIME WILL COST THE WORLD $10.5 TRILLION ANNUALLY BY 2025, UP FROM $6 TRILLION IN 2021, AND $3 TRILLION IN 2015”

There's ONE company behind most of the fake stats in InfoSec

THERE ARE 3.5 MILLION UNFILLED CYBERSECURITY JOBS GLOBALLY IN 2022

There's ONE company behind most of the fake stats in InfoSec

60% OF SMALL BUSINESSES GO OUT OF BUSINESS WITHIN 6 MONTHS OF A DATA BREACH

There's ONE company behind most of the fake stats in InfoSec

A TRIED AND TRUE PROCESS:

Make up a stat

Repeat it as much as possible

Get it published in as many places as possible

Recursive citations

Profit $$$

There's ONE company behind most of the fake stats in InfoSec

"...FEATURED AND QUOTED BY HUNDREDS OF..."

- major media outlets
- vendors
- academia
- governments
- associations
- event producers
- industry experts

There's ONE company behind most of the fake stats in InfoSec

“IT DOES EXACTLY WHAT IT'S DESIGNED TO. IT MAKES MONEY.”

— James McCormick, who sold £50m fake bomb detectors to countries like Iraq

2011

HBGary Federal

Distribute.IT

DigiNotar

2012

Only Honest

2014

Code Spaces

2016

MyBizHomepage

Precedent Communications

2018

Colorado Timberline

Vastaamo

The infamous “60% of small businesses…” stat

ONE OF THE MOST PROLIFIC AND LONG-LIVED FAKE STATS

The infamous “60% of small businesses...” stat

WAIT. 60%? OF ALL SMALL BUSINESSES BREACHED? THAT CAN'T BE RIGHT, CAN IT?

- If a small business goes under months after a breach, how do we know the breach was the cause?
- What percentage of small businesses go under across any 6 month period?
- Where did this data come from?

The infamous “60% of small businesses...” stat

WHERE'S THE EVIDENCE?

It didn't exist, so I started researching.

The infamous “60% of small businesses...” stat

THE DESTROYED BY BREACH DATASET

23 Companies - not last year, but ALL TIME

https://bit.ly/DestroyedByBreach

The infamous “60% of small businesses...” stat

StaySafeOnline.org
National Cyber Security Alliance

Symantec

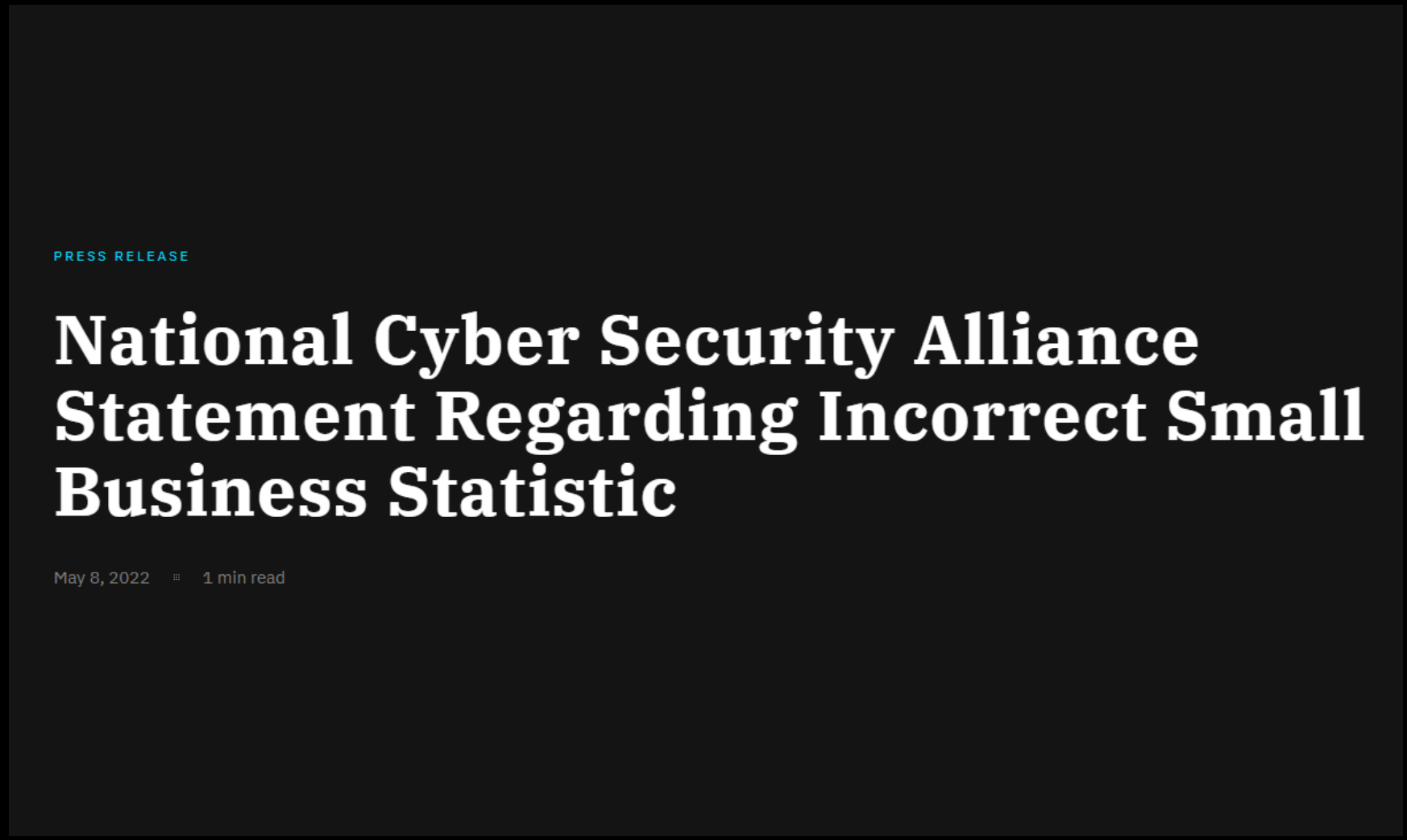
2011 NATIONAL SMALL BUSINESS STUDY

The National Cyber Security Alliance has conducted a new study with Symantec to analyze cyber security practices, behaviors and perceptions of small businesses throughout the United States. The study was conducted by Zogby International, which polled 1,045 U.S. small business owners from September 19-21, 2011. The survey had a margin of +/- 3.1 percentage points. Key findings of this study are listed below:

WHERE DID IT COME FROM?

The National Cyber Security Alliance (as StaySafeOnline) once referenced this stat for 6 months, before pulling the reference and posting a retraction and apology.

The infamous “60% of small businesses…” stat



PRESS RELEASE

National Cyber Security Alliance Statement Regarding Incorrect Small Business Statistic

May 8, 2022 · 1 min read

The infamous “60% of small businesses...” stat

How a Fake Cyber Statistic Raced Through Washington

SEAN PAVONE/SHUTTERSTOCK.COM

By Joseph Marks,
Senior Correspondent

MAY 3, 2017

A frequently cited statistic about the danger small businesses face from cyberattacks has no basis in fact.

Editor's note: This article was updated with comments from Sen. Brian Schatz's office and NIST.

JOSEPH MARKS AT NEXTGOV TRACKED DOWN THE SOURCE

“[the source] told Nextgov he believes the figure was provided by a cybersecurity expert he interviewed for the story but cannot recall the expert’s name more than five years later.”

The infamous “60% of small businesses…” stat

LEGACY: MORE POPULAR THAN EVER

- The source is still regularly using the fake stat
- Has been quoted by the SEC and entered into congressional testimony
- Led to the NIST Small Business Cybersecurity Act (HR 2105)
- Vendors using it
- Thought leaders using it

2011

HBGary Federal

Distribute.IT

DigiNotar

2012

Only Honest

2014

Code Spaces

2016

MyBizHomepage

Precedent Communications

2018

Colorado Timberline

Vastaamo

2019

Brookside ENT

AMCA

United Structures of America

PM Consultants

Wood Ranch Medical

The Heritage Company

2020

Best Medical Transcription

Levitas Capital

2021

NoSupportLinuxHosting

Demotivational myths and maxims

ATTACKERS ONLY NEED TO GET IT RIGHT ONCE, DEFENDERS HAVE TO GET IT RIGHT EVERY TIME

This is only true for the attacker's initial foothold

Then the math flips (most attacks require multiple steps)

Now the attacker has to get it right every time

Or risk getting caught and removed

Defenders have the home (alone) advantage

Don't make environments easy for attackers to navigate

Demotivational myths and maxims

IT'S NOT IF YOU GET HACKED, IT'S WHEN

Verizon DBIR: “incidents” and “breaches” aren't the same

Incidents happen often, but don't have to become breaches

What's the message here? Might as well give up?

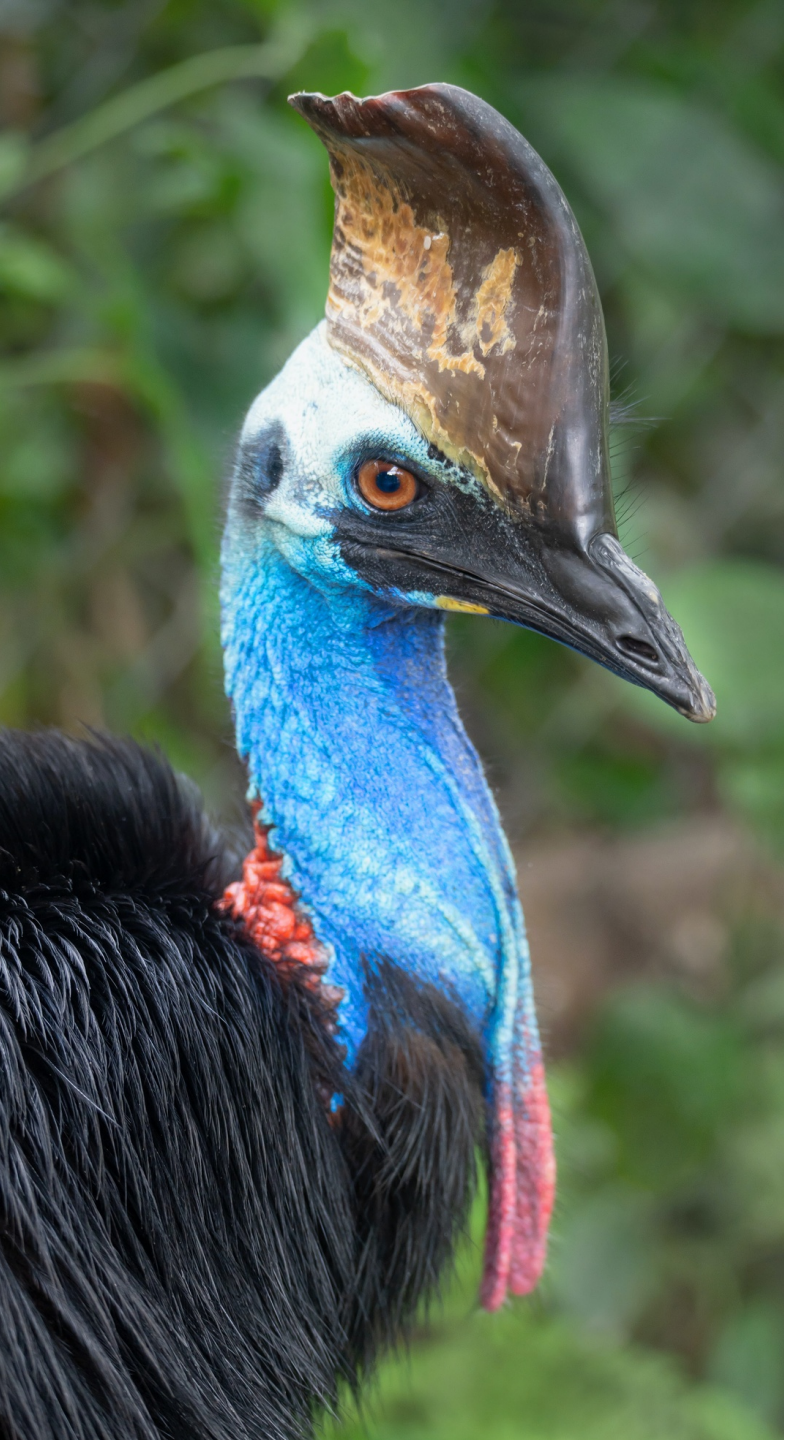
Most often heard from someone trying to sell something

Demotivational myths and maxims

HUMANS ARE THE WEAKEST LINK IN SECURITY

Humans are reliably unreliable -- Lisa Plaggemier

https://bit.ly/CyberBS



HEALTHY SKEPTICISM

Look up stats. Find data that provides context and sanity checks for myths and stats.

NO DATA, NO METHODOLOGY, NO TRUST

Reports without data, a stated methodology, or legitimate citations don't deserve your trust. There's plenty of good research out there, don't waste your time.

FLIP THE SCRIPT: MOTIVATIONAL MAXIMS

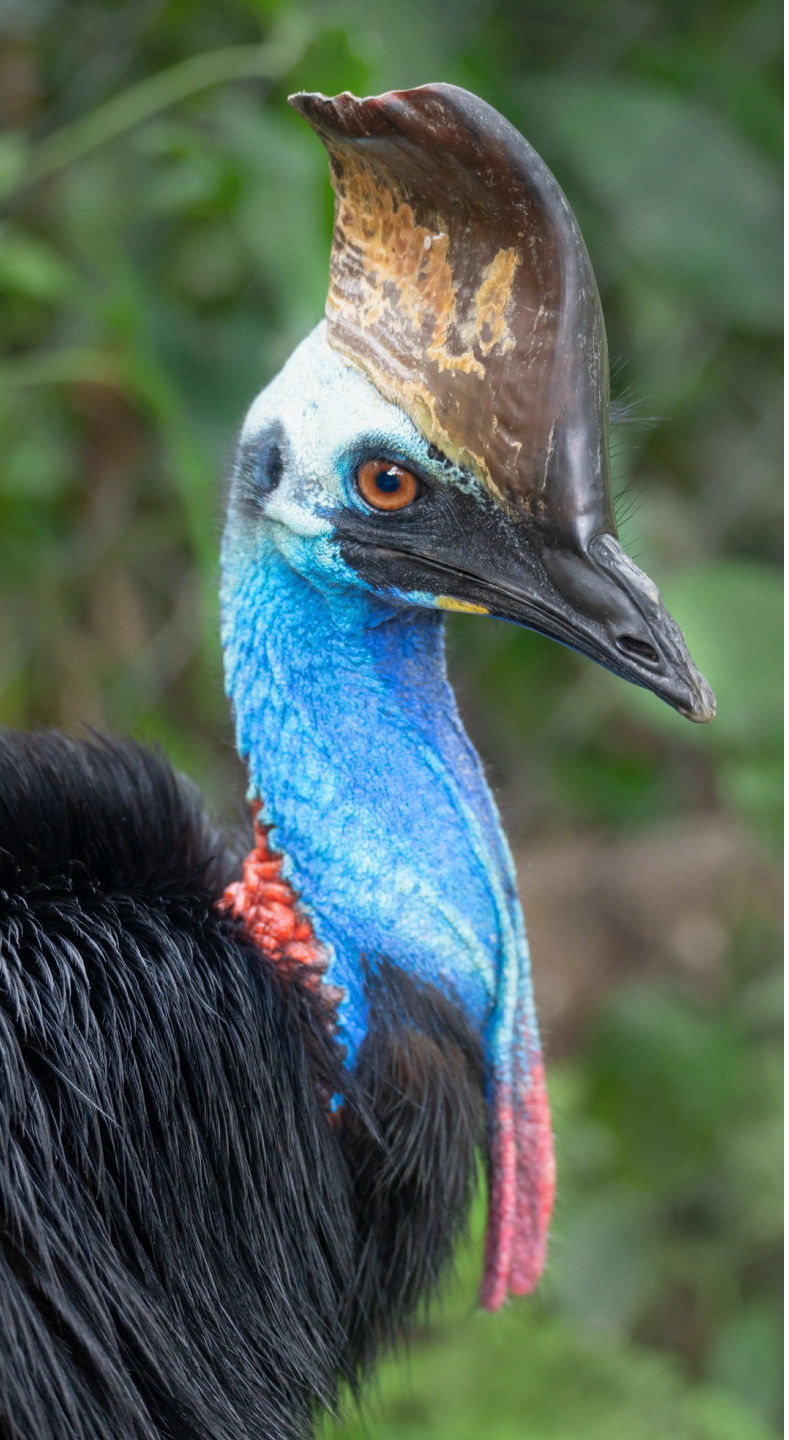
Let's replace these stereotypical sayings and spread more truth.

FIND THE DATA, SHARE THE DATA

Find and collect data - you'd be surprised how much is available

Ask nicely (the DBIR folks are very accommodating, for example)

Failing all that, gather the data yourself & share with others



DON'T ACCUSE, ASSIST

Don't just call out fake stats and those that use them - allow them to save face: have the correct numbers or alternatives readily available.

INCLUDE REFERENCES

Don't use data without sharing the source. Make survey sizes clear (e.g. n=205).

USE STATISTICS TO INFORM AND EDUCATE

Instead of using stats as a statement, or a blunt tool, think of them as the beginning of a conversation, or a teaser for a deeper discussion.

SHARE YOUR OWN RESEARCH

The data you're looking for doesn't exist? How would you go about gathering it yourself? Commission a survey? Hire some researchers?

the truth is worth it

Add time to check facts and figures

friends don't let friends use fake stats

your employees, customers, and audience will thank you

Adrian Sanabria (@sawaba)