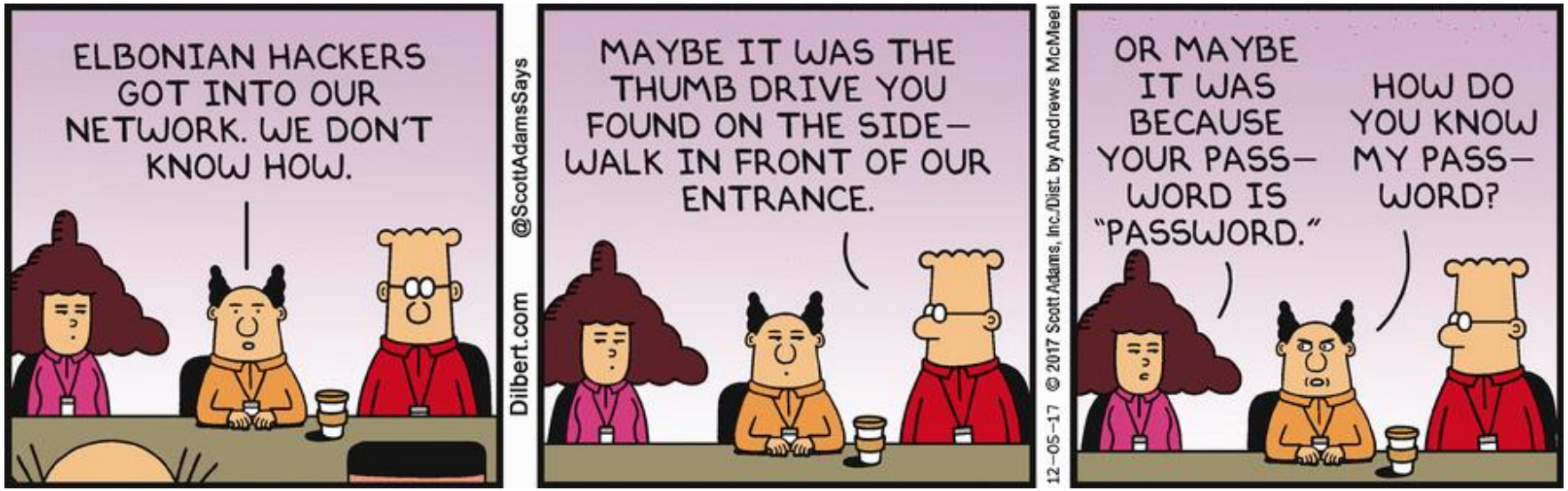
Australian National University

Cybersecurity and Phishing



Web Development and Design
Comp1710/6780
Week 7, Monday 19 August 2022

Dr Sabrina Caldwell
Human Centred Computing
The Australian National University,
Research School of Computer Science

Why is online security important?

INTEGRITY

2007

United Nations website hacked to appear to be protesting US and Israeli policies in the Middle East.

HACKED BY KEREM125 MOSTED AND GSY THAT IS CYBERPROTEST HEY YSRAIL AND USA DON'T KILL CHILDREN AND OTHER PEOPLE PEACE FOR EVER NO WAR

Biggest data breach known so far

Date: 2013-14
Impact: 3 billion user accounts

Reported 2016: 'State-sponsored actor' steals data of 500M users

Details: In September 2016, the once dominant Internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by "a state-sponsored actor," in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of **500 million** users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm.

Reported 2017: 'State-sponsored actor' actually stole data of *ALL* Yahoo! Users – 3Bn

Details: A couple of months later, in December, it buried that earlier record with the disclosure that a breach in 2013, by a different group of hackers had compromised **1 billion** accounts. Besides names, dates of birth, email addresses and passwords that were not as well protected as those involved in 2014, security questions and answers were also compromised. In October of 2017, Yahoo revised that estimate, saying that, in fact, **all 3 billion user accounts** had been compromised.

Cybersecurity – improper data sharing

2018: > 87 million Facebook users' data improperly shared

Aleksandr Kogan harvested the data for use of Cambridge Analytica, who used it for psychographic profiles of users to deploy targeted political ads during the 2016 US presidential election (Trump's chief strategist was VP of Cambridge Analytica)

Kogan now admits what he did wasn't right.

Facebook banned Cambridge Analytica in March.

Facebook boss Mark Zuckerberg says his own data was shared with Cambridge Analytica

Updated 12 Apr 2018, 1:56pm

VIDEO: Mr Zuckerberg admits his data was improperly used (Photo: AP/Andrew Harnik) (ABC News)

Facebook CEO Mark Zuckerberg has revealed during a second day of sparring with US politicians over privacy concerns that he was among the 87 million users whose data was improperly shared.

RELATED STORY: Facebook is in an AI 'arms race' with Russia, Zuckerberg tells US senators

RELATED STORY: Use Facebook? Here's how to check right now if Cambridge Analytica got your data

RELATED STORY: Australia is looking into the breach of 300,000 Facebook users' data

http://www.abc.net.au/news/2018-04-12/zuckerberg-says-his-own-data-was-shared-with-cambridge-analytica/9643212

Threat environment ($$$)

Cyber security is considered a global challenge and a matter of national priority

The Australian Crime Commission (ACC) estimates that **cyber crime costs Australia $1 billion annually**

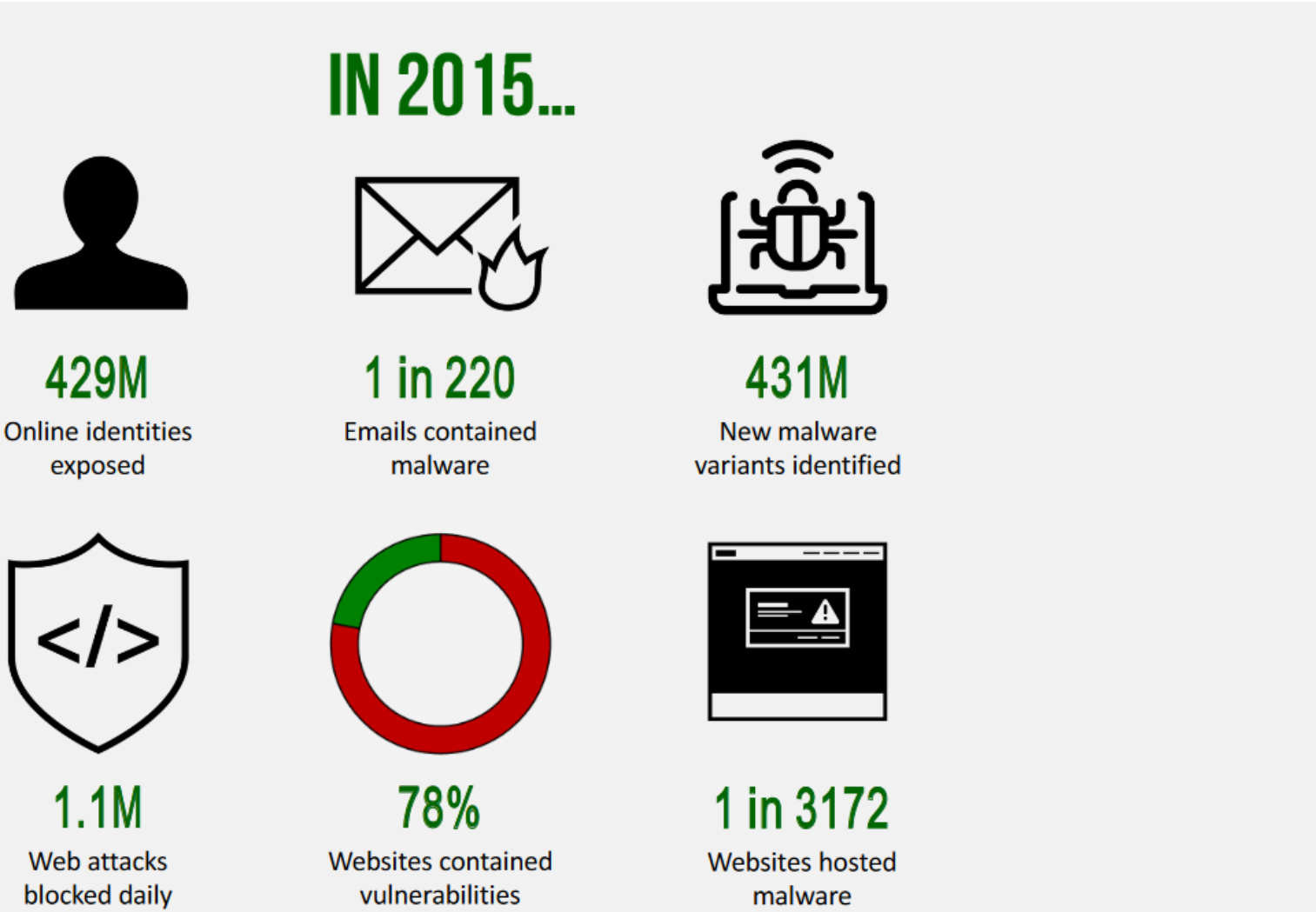
In 2016 Australian Government launched a new Cyber Security strategy investing more than $230 million over four years. Active cybersecurity departments are now embedded in many government organisations

https://www.investsmart.com.au/investment-news/a-cash-strategy-for-smsfs/138831

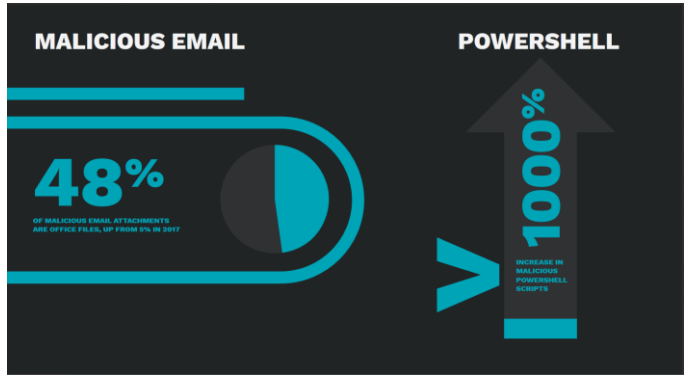
Symantec Internet Security Threat Report 2016

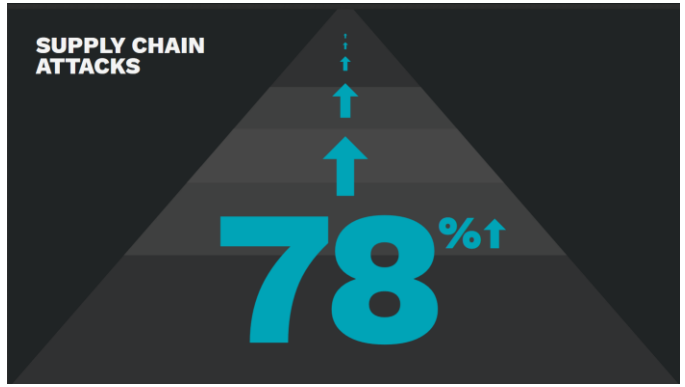
In **2019** the strongest trend in cyber attacks was **malicious Powershell* script attacks** up **1,000%**

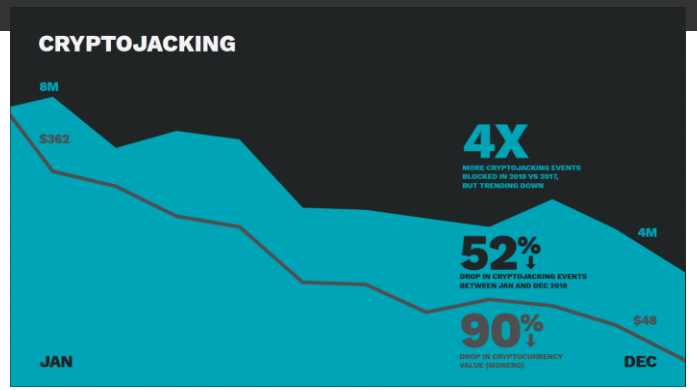
*Powershell is a Windows scripting language for running admin tasks

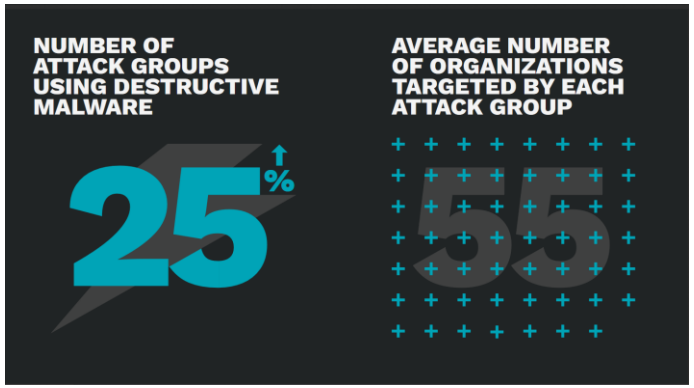


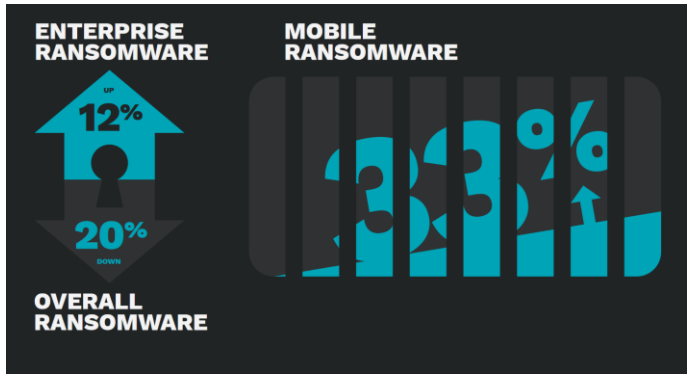
in 2019 …


MALICIOUS EMAIL
48%
OF MALICIOUS EMAIL ATTACHMENTS ARE OFFICE FILES, UP FROM 5% IN 2017
POWERSHELL
1000%
INCREASE IN MALICIOUS POWERSHELL SCRIPTS


SUPPLY CHAIN ATTACKS
78%

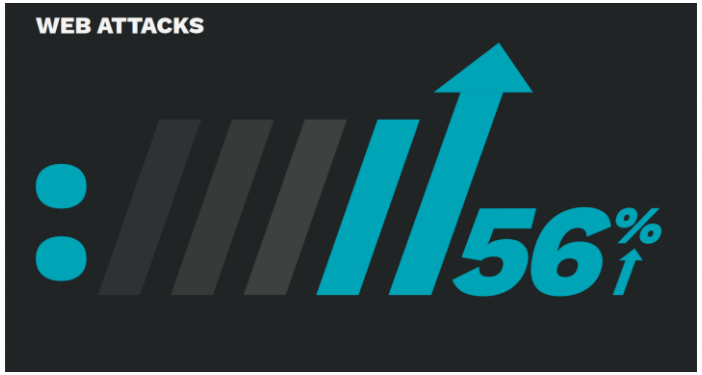

CRYPTOJACKING
8M
$362
4X
MORE CRYPTOJACKING EVENTS BLOCKED IN 2018 VS 2017, BUT TRENDING DOWN
4M
52%
DROP IN CRYPTOJACKING EVENTS BETWEEN JAN AND DEC 2018
90%
DROP IN CRYPTOCURRENCY VALUE (MONERO)
$48
JAN
DEC


NUMBER OF ATTACK GROUPS USING DESTRUCTIVE MALWARE
25%
AVERAGE NUMBER OF ORGANIZATIONS TARGETED BY EACH ATTACK GROUP
55


ENTERPRISE RANSOMWARE
UP
12%
20%
DOWN
OVERALL RANSOMWARE
MOBILE RANSOMWARE
33%


MALICIOUS URLS
ONE IN TEN
URLS ARE MALICIOUS

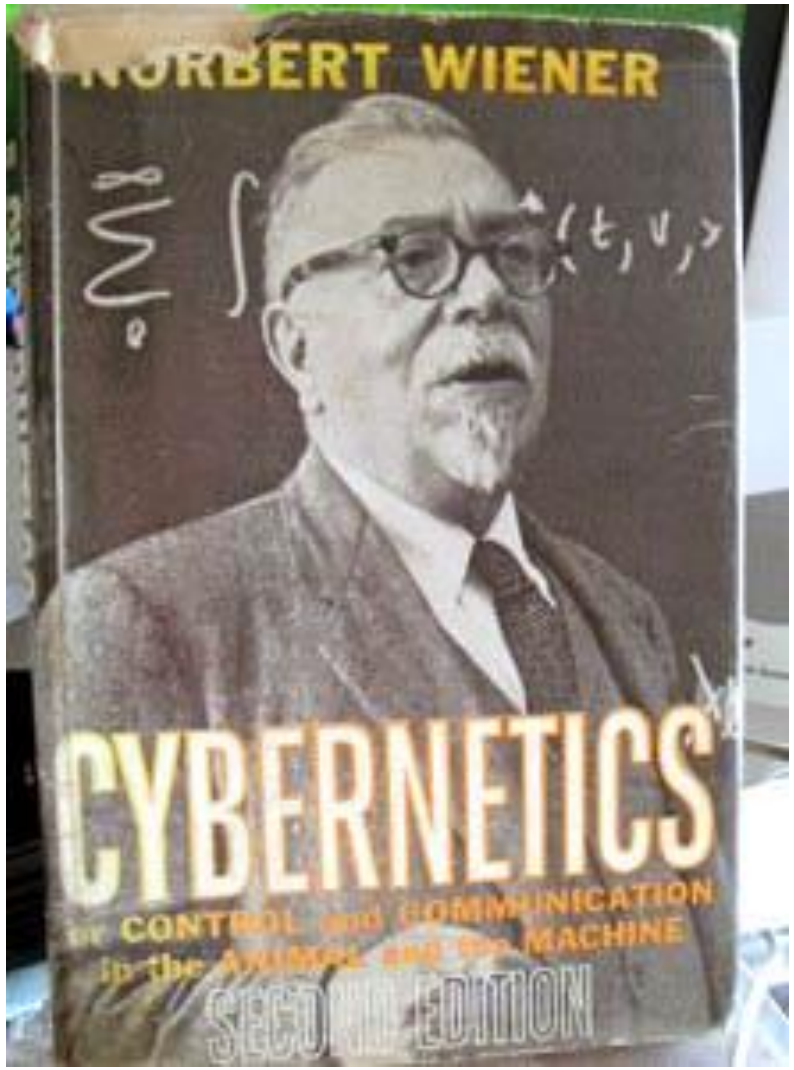

FORMJACKING ATTACKS
4,800
AVERAGE NUMBER OF WEBSITES COMPROMISED WITH FORMJACKING CODE EACH MONTH
BLOCKED
FORMJACKING ATTACKS ON ENDPOINTS
3.7M


WEB ATTACKS
56%

BUT LOCALLY...

Web sites and applications are particularly vulnerable

Users themselves are also targeted



http://laroucheplanet.info/pmwiki/pmwiki.php?n=Library.WienerWorld

What is cyber security anyway?

1940s Cybernetics

Study of communication and control systems
in living beings and machines

Oxford dictionary: Cybernetics is from Greek word
kubernētēs (κυβερνᾶν), steersman, from *kubernan* 'to steer'

1960s – 1990s cyber- and cyb-

Cybernetics shortened to form new words
(cyberfriend, cyberspace, cyborg, cyberbullying)

Gartner, 2013: "Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries."

Oxford definition of cybernetics/cyber - https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/
Gartner: http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

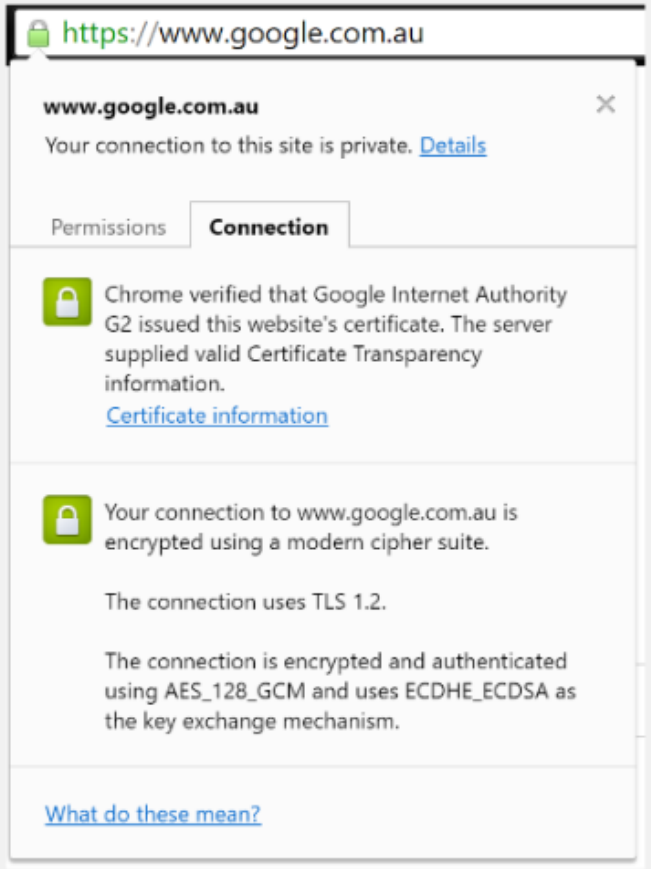
Why is online security important?

Confidentiality
Ensuring user privacy

Availability
Ensuring the service is available to users

Integrity
Protecting branding against defacement

CONFIDENTIALITY & Non-repudiation



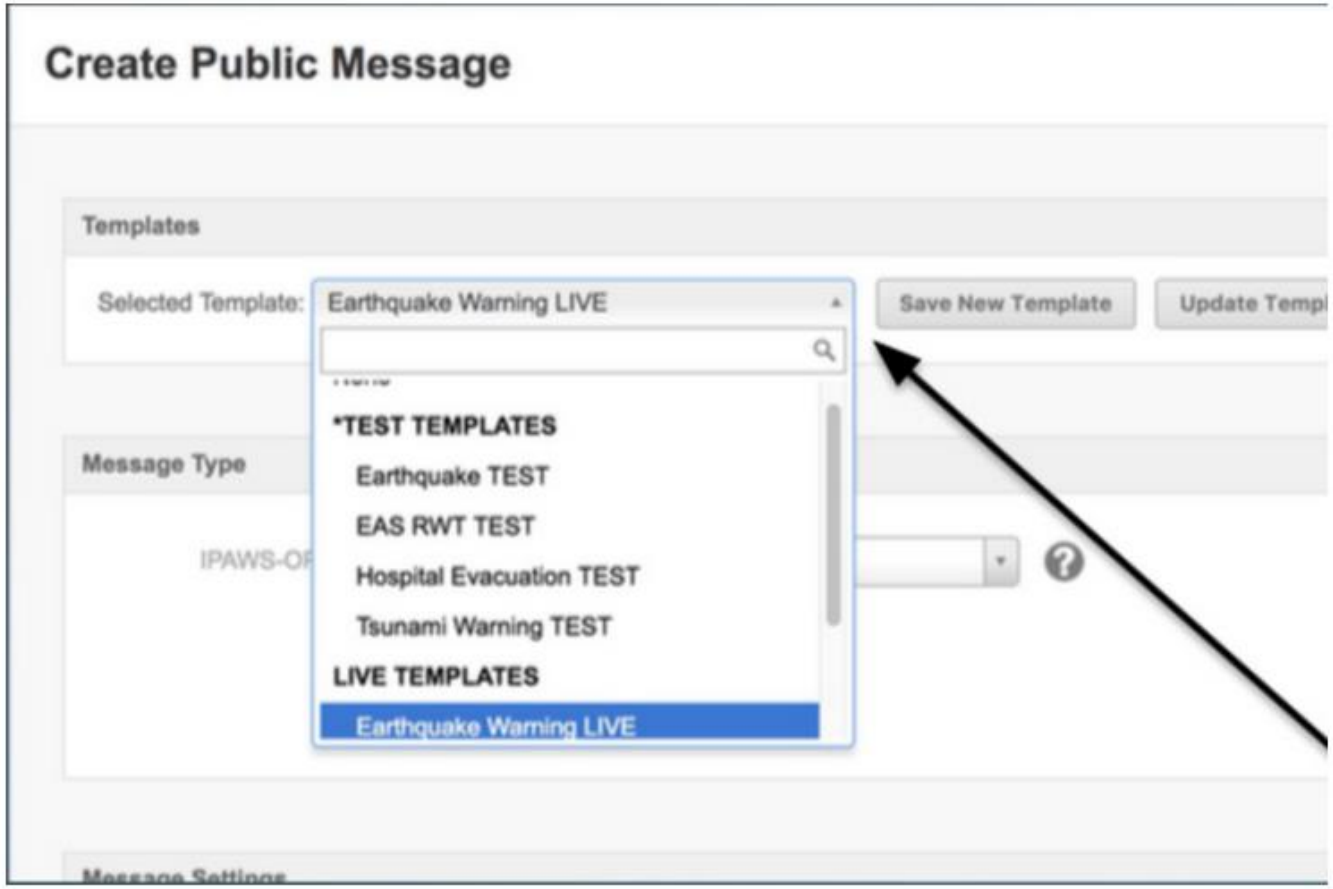
aka 'Trust'

Cybersecurity – Small mistakes with big consequences

January 2018

Residents of Hawaii terrified by live warning of incoming ballistic missiles.

Took 38 minutes before alert was retracted.



Major design failure: USA FEMA-approved AlertSense software developer designs software that's easy to get really wrong.

https://www.theverge.com/2018/1/18/16905512/hawaii-missile-software-false-alarm-emergency-alert

Why should I care?

Security is everyone's problem

New vulnerabilities are discovered daily

As web developers, you must be aware of these issues and build security into your website and applications

vulnerabilities

A vulnerability is a weakness in an application that may allow a malicious entity to cause harm

Vulnerabilities are generally caused by a design flaw or implementation bug

Again: new vulnerabilities are discovered daily!

Evelyn Simak / Gap in fence

Common web attacks

An attack is a technique used to exploit a vulnerability

Brute forcing (hit and try until you crack password or find hidden pages/content)
Injections (attacker puts malevolent code in query string of an HTTP request)
SQL Injection (attacker injects malevolent code in data driven websites)
XSS (cross site scripting injects malicious scripts into trusted websites that then forwards the input)

Spoofing (attacker supplies content to a web application; can shift user to fake site)
Denial of Service (flooding a site with requests to stop legitimate users)
CSRF (cross-site request forgery – forcing/tricking users into performing tasks (like transferring funds or changing their email))
Man-in-the-middle (intercept and interfere with communications between user and legitimate server)
Social engineering (psychological manipulation to trick users into making security mistakes or giving away information)

What can you do?

Learn and understand

Code securely; be aware of security implications

Test your code as part of the web development process

… more on this next week.