# Cybersecurity in the Fire Alarm Industry

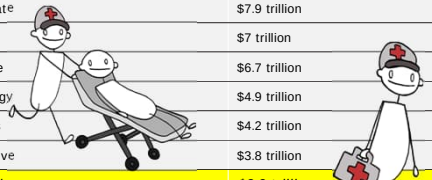
## Protecting Critical Systems

Ben Adams
President of Field Sim
Founder of FireAlarm.Training

Automatic Fire Alarm Association

1

| Rank | Industry | Estimated Global Revenue/Impact (2023) |
|---|---|---|
| 1 | Healthcare | $10 trillion |
| 2 | Consumer Packaged Goods | $8 trillion |
| 3 | Real Estate | $7.9 trillion |
| 4 | Banking | $7 trillion |
| 5 | Insurance | $6.7 trillion |
| 6 | Technology | $4.9 trillion |
| 7 | Oil & Gas | $4.2 trillion |
| 8 | Automotive | $3.8 trillion |
| *9* | *Cybercrime* | *$3.2 trillion* |
| 10 | Drug Trafficking | $500 billion |

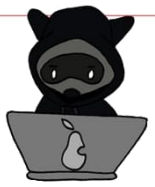


Automatic Fire Alarm Association

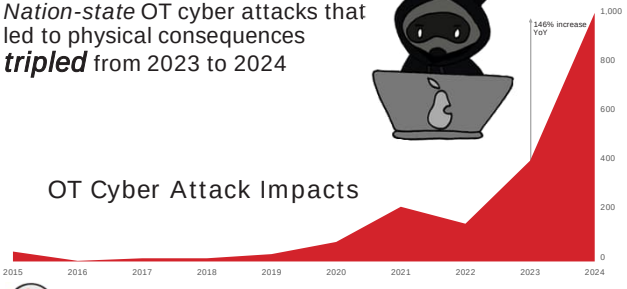
Source: World Health System Facts, The Sterling Choice, Research and Markets, McKinsey, Allianz, Gartner, IBISWorld, Automotive Industries, FBI Internet Crime Complaint Center, Into the Web of Profit (Dr Michael McGuire), The Economist, and Global Financial Integrity

2

*Nation-state* OT cyber attacks that led to physical consequences ***tripled*** from 2023 to 2024



OT Cyber Attack Impacts




Automatic Fire Alarm Association

Source: Waterfall Security 2025 OT Cyber Security Threat Report

3

## Why fire alarm systems are targets

Automatic Fire Alarm Association

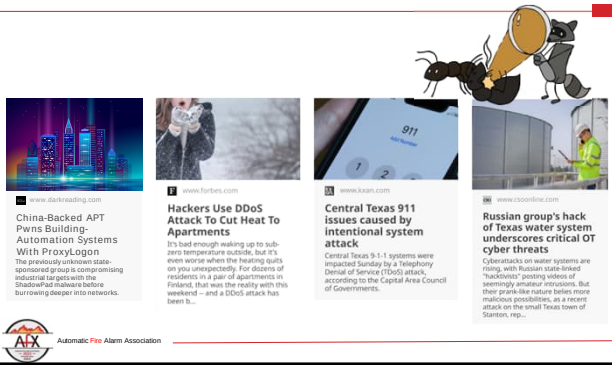
4

## The average ransomware payment in 2024 was

# $2 million

Automatic Fire Alarm Association
Source: Sophos State of Ransomware 2024

5



www.darkreading.com

China-Backed APT Pwns Building-Automation Systems With ProxyLogon

The previously unknown state-sponsored group is compromising industrial targets with the ShadowPad malware before burrowing deeper into networks.

www.forbes.com

**Hackers Use DDoS Attack To Cut Heat To Apartments**

It's bad enough waking up to sub-zero temperature outside, but it's even worse when the heating quits on you unexpectedly. For dozens of residents in a pair of apartments in Finland, that was the reality with this weekend – and a DDoS attack has been b...

www.kxan.com

**Central Texas 911 issues caused by intentional system attack**

Central Texas 9-1-1 systems were impacted Sunday by a Telephony Denial of Service (TDoS) attack, according to the Capital Area Council of Governments.

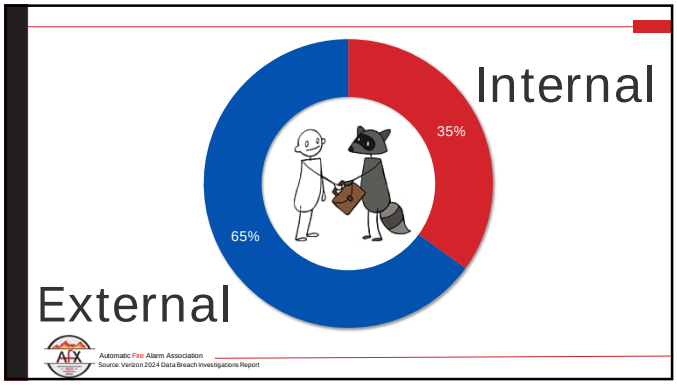
www.cscoonline.com

**Russian group's hack of Texas water system underscores critical OT cyber threats**

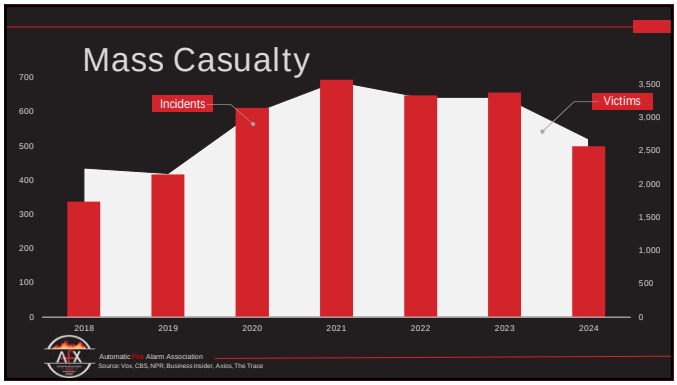
Cyberattacks on water systems are rising, with Russian state-linked "hacktivists" posting videos of seemingly amateur intrusions. But their prank-like nature belies more malicious possibilities, as a recent attack on the small Texas town of Stanton, rep...

Automatic Fire Alarm Association

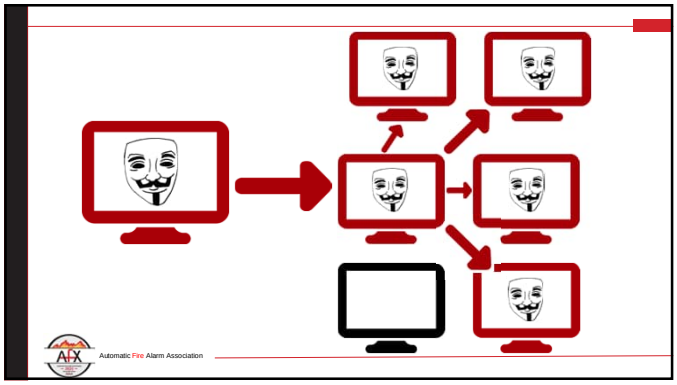
6


Internal
35%
65%
External
Automatic Fire Alarm Association
Source: Verizon 2024 Data Breach Investigations Report

7

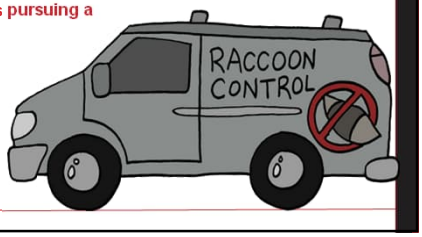

Mass Casualty
Incidents
Victims
700
600
500
400
300
200
100
0
3,500
3,000
2,500
2,000
1,500
1,000
500
0
2018
2019
2020
2021
2022
2023
2024
Automatic Fire Alarm Association
Source: Vox, CBS, NPR, Business Insider, Axios, The Trace

8


Automatic Fire Alarm Association

9

The fire alarm industry is pursuing a secure future




Automatic Fire Alarm Association

10

## NFPA 72 Ch 11 *Rules for fire alarm equipment that connects to a network*

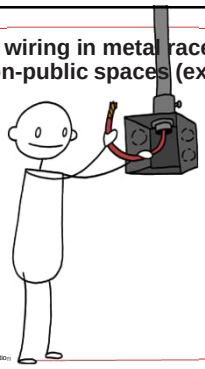
| | Non-IP Wired | Non-IP Wireless or IP but not Publicly Accessible | Publicly Accessible IP |
|---|---|---|---|
| Security Level 3 | | | |
| Security Level 2 | | | |
| Security Level 1 | | | |

Automatic Fire Alarm Association

*IP = Internet Protocol

11

## Run network wiring in metal raceway, metal armored cables, or non-public spaces (exception for SL1)



Automatic Fire Alarm Association

12

NFPA 72 Ch 11

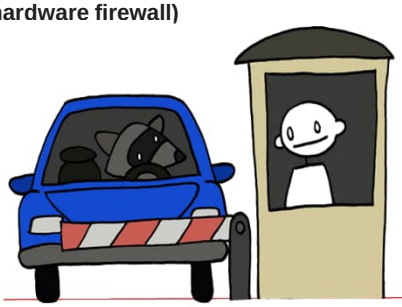
*Rules for All Security Levels*

SL

Automatic Fire Alarm Association

13

**Only connect to external networks via security gateway (i.e., hardware firewall)**



Automatic Fire Alarm Association

14

**Protect unused physical data ports on fire alarm equipment**

Automatic Fire Alarm Association

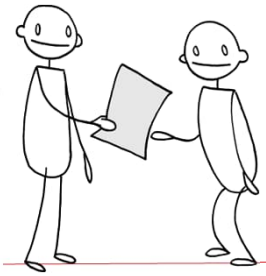
15

**Document which security level has been applied, and which standards were used in support of it**

Automatic Fire Alarm Association

16

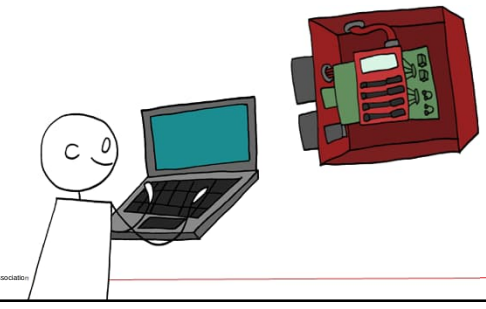
**Provide building owner/manager's contact info to the manufacturer**



Automatic Fire Alarm Association

17

**Install software and firmware updates**



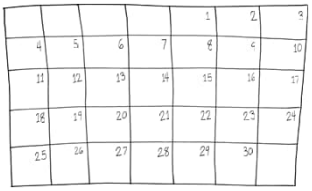
Automatic Fire Alarm Association

18

## Annual Verifications

Equipment cybersecurity certificates are still valid

Manufacturer(s) have up-to-date contact info for the building owner/manager



Automatic Fire Alarm Association

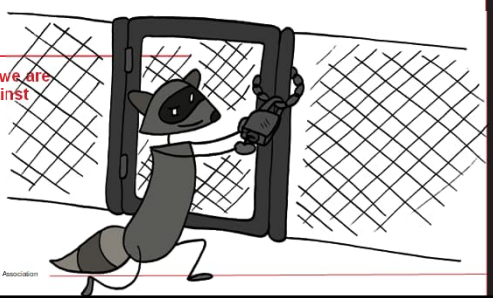
19

## Implement deployment plans and change control committee (ref. 26.6.3)

Automatic Fire Alarm Association

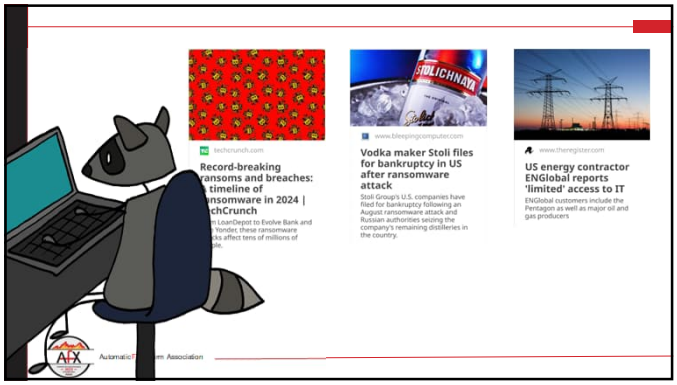
20

**The dangers we are guarding against**

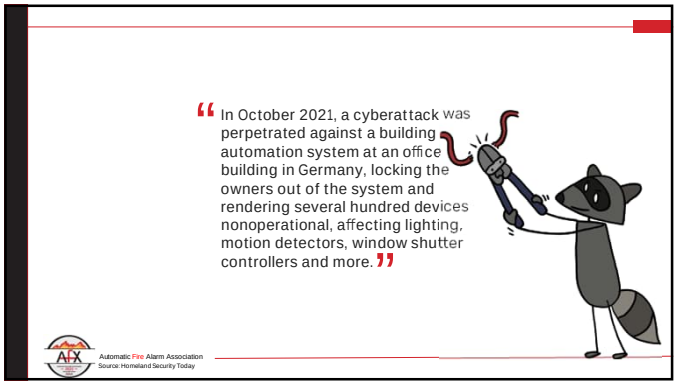


Automatic Fire Alarm Association

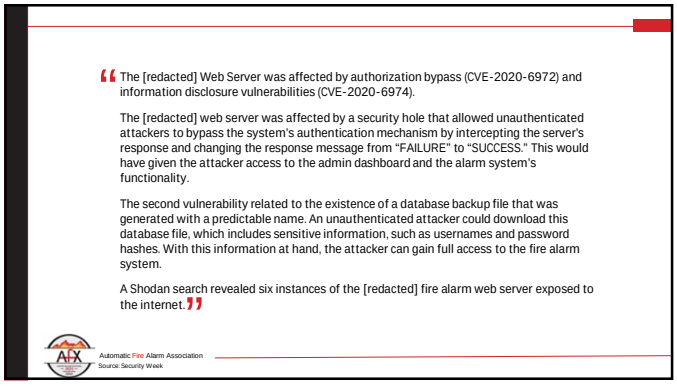
21


techcrunch.com
Record-breaking ransoms and breaches: timeline of ransomware in 2024 | TechCrunch
www.bleepingcomputer.com
Vodka maker Stoli files for bankruptcy in US after ransomware attack
Stoli Group's U.S. companies have filed for bankruptcy following an August ransomware attack and Russian authorities seizing the company's remaining distilleries in the country.
www.theregister.com
US energy contractor ENGlobal reports 'limited' access to IT
ENGlobal customers include the Pentagon as well as major oil and gas producers
Automatic Fire Alarm Association

22


“In October 2021, a cyberattack was perpetrated against a building automation system at an office building in Germany, locking the owners out of the system and rendering several hundred devices nonoperational, affecting lighting, motion detectors, window shutter controllers and more.”
Automatic Fire Alarm Association
Source: Homeland Security Today

23


“The [redacted] Web Server was affected by authorization bypass (CVE-2020-6972) and information disclosure vulnerabilities (CVE-2020-6974).
The [redacted] web server was affected by a security hole that allowed unauthenticated attackers to bypass the system's authentication mechanism by intercepting the server's response and changing the response message from "FAILURE" to "SUCCESS." This would have given the attacker access to the admin dashboard and the alarm system's functionality.
The second vulnerability related to the existence of a database backup file that was generated with a predictable name. An unauthenticated attacker could download this database file, which includes sensitive information, such as usernames and password hashes. With this information at hand, the attacker can gain full access to the fire alarm system.
A Shodan search revealed six instances of the [redacted] fire alarm web server exposed to the internet.”
Automatic Fire Alarm Association
Source: Security Week

24

## Integrators

Concrete steps to protect life safety systems from cyber attacks

Automatic Fire Alarm Association

25

## Use unique passwords for every fire alarm system

Automatic Fire Alarm Association

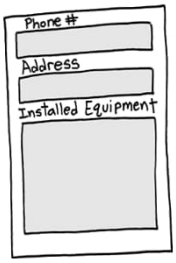
26

## Keep fire alarm system firmware and software and all the software on your computer/phone updated

Automatic Fire Alarm Association

27

**Facilitate the manufacturer's need to track contact info for the building owner/manager**




Automatic Fire Alarm Association

28

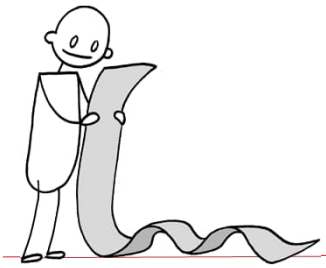
**Building Owners and Managers**

**Concrete steps to protect life safety systems from cyber attacks**

Automatic Fire Alarm Association

29

**Make sure regular security updates are included in your service agreement**



Automatic Fire Alarm Association

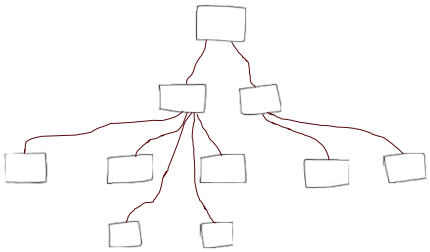
30

## Make sure the FACU isn't left at the default password

Automatic Fire Alarm Association

31

## Provide a dedicated OT network if you have internet-connected fire alarm systems

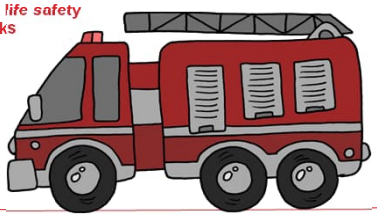


Automatic Fire Alarm Association

32

## AHJs

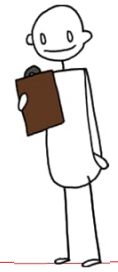
**Concrete steps to protect *life safety* systems from cyber attacks**



Automatic Fire Alarm Association

33

## Ask for evidence of cybersecurity measures



Automatic Fire Alarm Association

34

## Have integrator disclose the latest and the currently installed firmware versions for system components

Installed Version

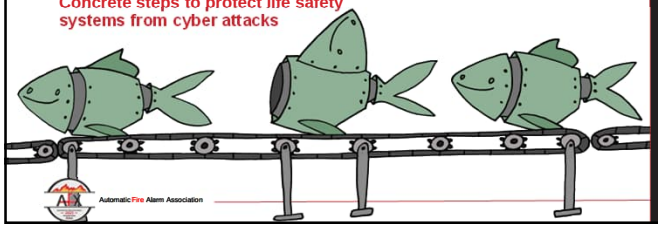
Latest Version

Automatic Fire Alarm Association

35

## Manufacturers

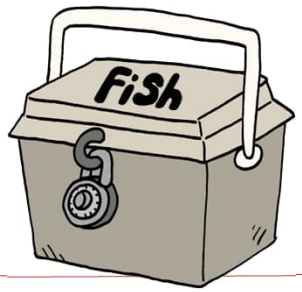
**Concrete steps to protect life safety systems from cyber attacks**



Automatic Fire Alarm Association

36

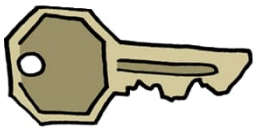
## Implement security measures to protect programming access






37

## Ship hardware with unique passwords





38

## Don't use a S/N or MAC address as the password

E8:39:6F:B7



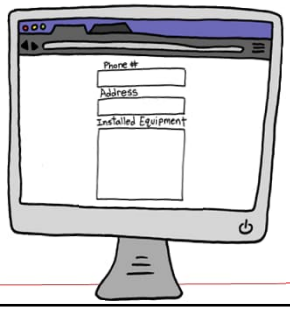
39

**Don't print any part of the credentials on the outside of the box**

Automatic Fire Alarm Association

40

**Make it easy (yet secure) for end user contact info to be updated**




Automatic Fire Alarm Association

41

**Notify your integrators and building representatives of security updates**

Automatic Fire Alarm Association

42

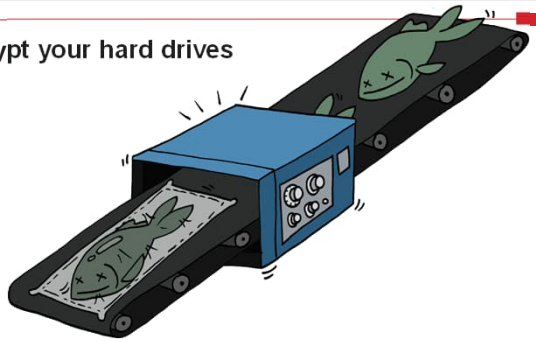
## Everyone

**Concrete steps to protect life safety systems from cyber attacks**

Automatic Fire Alarm Association

43

## Encrypt your hard drives



Automatic Fire Alarm Association

44

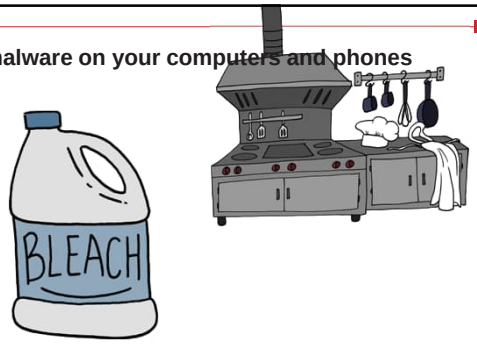
## Use *paid** VPN when connecting to untrusted Wi-Fi

*If you're not the customer, you're the product

Automatic Fire Alarm Association

45

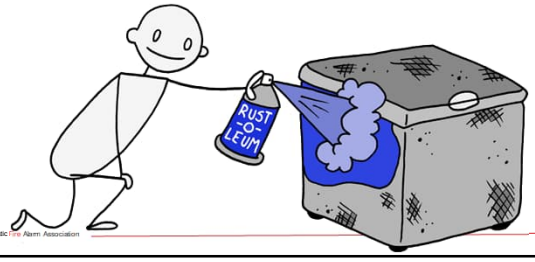
## Use antimalware on your computers and phones






46

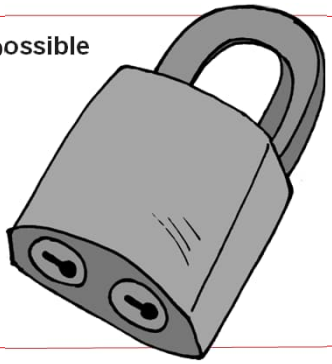
## Apply security updates to your computers and phone regularly






47

## Use MFA where possible

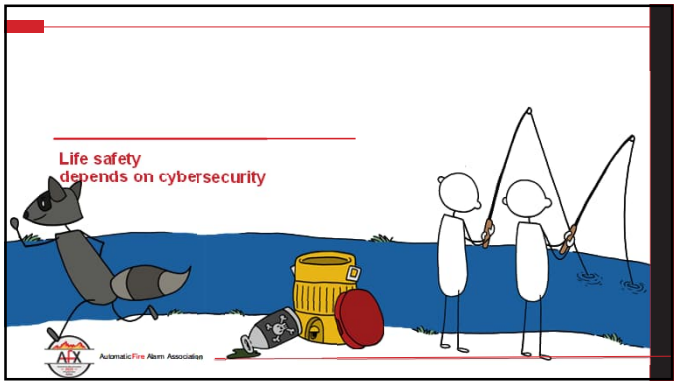




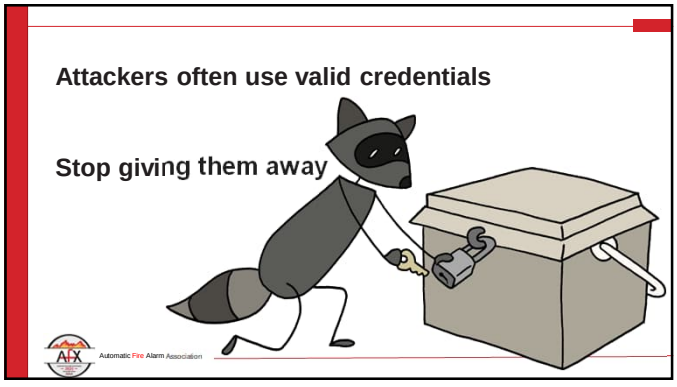
48

| | 2024 | | 2034 (Projected) | | 2044 (Projected) | |
|---|---|---|---|---|---|---|
| Length | Time to Crack | Cost to Crack | Time to Crack | Cost to Crack | Time to Crack | Cost to Crack |
| 1 | Instant | $0 | Instant | $0 | Instant | $0 |
| 2 | Instant | $0 | Instant | $0 | Instant | $0 |
| 3 | Instant | $0 | Instant | $0 | Instant | $0 |
| 4 | Instant | $0 | Instant | $0 | Instant | $0 |
| 5 | Instant | $0 | Instant | $0 | Instant | $0 |
| 6 | Instant | $0 | Instant | $0 | Instant | $0 |
| 7 | 1.75 seconds | $0 | Instant | $0 | Instant | $0 |
| 8 | 3 minutes | $7 | 5.14 seconds | $0 | Instant | $0 |
| 9 | 4 hours | $631 | 8 minutes | $0 | 15.11 seconds | $0 |
| 10 | 17 days | $59,326 | 13 hours | $31 | 24 minutes | $3 |
| 11 | 4 yr | $5 million | 49 days | $2,905 | 2 days | $290 |
| *12* | *407 yr* | *$524 million* | *13 yr* | *$273,025* | *145 days* | *$27,302* |
| 13 | 38,297 yr | $49 billion | 1,197 yr | $25 million | 37 yr | $2 million |
| 14 | 3 million yr | $4 trillion | 112,497 yr | $2 billion | 3,516 yr | $241 million |
| 15 | 338 million yr | $435 trillion | 10 million yr | $226 billion | 330,461 yr | $22 billion |
| 16 | 31 billion yr | $40 quadrillion | 994 million yr | $21 trillion | 31 million yr | $2 trillion |
| 17 | 2 trillion yr | $3 quintillion | 93 billion yr | $2 quadrillion | 2 billion yr | $200 trillion |
| 18 | 281 trillion yr | $361 quintillion | 8 trillion yr | $188 quadrillion | 274 billion yr | $18 quadrillion |
| 19 | 26 quadrillion yr | $33 sextillion | 825 trillion yr | $17 quintillion | 25 trillion yr | $1 quintillion |
| 20 | 2 quintillion yr | $3 septillion | 77 quadrillion yr | $1 sextillion | 2 quadrillion yr | $166 quintillion |

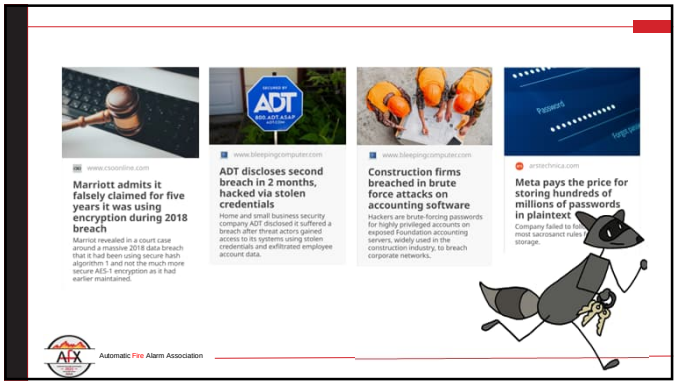
49




50



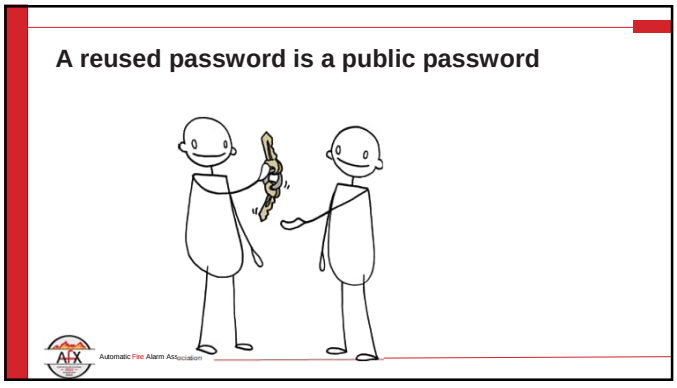

51


www.csoonline.com
Marriott admits it falsely claimed for five years it was using encryption during 2018 breach
Marriot revealed in a court case around a massive 2018 data breach that it had been using secure hash algorithm 1 and not the much more secure AES-1 encryption as it had earlier maintained.
www.bleepingcomputer.com
ADT discloses second breach in 2 months, hacked via stolen credentials
Home and small business security company ADT disclosed it suffered a breach after threat actors gained access to its systems using stolen credentials and exfiltrated employee account data.
www.bleepingcomputer.com
Construction firms breached in brute force attacks on accounting software
Hackers are brute-forcing passwords for highly privileged accounts on exposed Foundation accounting servers, widely used in the construction industry, to breach corporate networks.
arstechnica.com
Meta pays the price for storing hundreds of millions of passwords in plaintext
Company failed to fe
most sacrosanct rules
storage.
Automatic Fire Alarm Association

52

How many digital accounts do you have?
Automatic Fire Alarm Association

53


A reused password is a public password
Automatic Fire Alarm Association

54

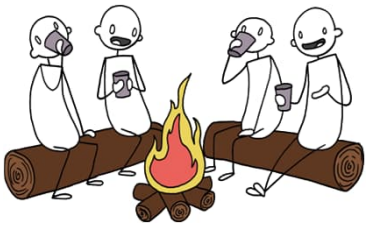
**Create a task right now to start using a password manager with long, unique passwords**

- [ ] Setup Password Manager
- [ ] Change Passwords
- [ ]
- [ ]
- [ ]

Automatic Fire Alarm Association

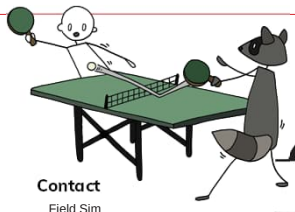
55

**By protecting fire alarm systems from cyber attacks, you're protecting people's lives**



Automatic Fire Alarm Association

56



## Questions

**Contact**

Field Sim
Ben Adams
ben@fieldsim.com

Or use the form at the bottom of every page
HTTPS://FIREALARM.TRAINING

Free cybersecurity resources:
HTTPS://TRAINING.FIELDSIM.COM/AFX2025

Automatic Fire Alarm Association

57