Security Awareness is Dead
Long Live Security Awareness

Dr Jessica Barker  |  Co-Founder  |  Redacted Firm
Top university under 'ransomware' cyber-attack
By Sean Goddard
Published on May 1, 2017

One in three universities ‘face cyber attacks every hour’
Nearly half of those surveyed said exam results had been infiltrated with over three in five claiming that students pose a threat to data.

UK universities targeted by cyber-thieves
5 August 2017

Cyberattack 101: Why Hackers Are Going After Universities
By Emily Adamczyk and Susan H. Brill / Aug 1, 2017 / 12:15 PM ET / Updated Aug 2, 2017 / 12:15 PM ET

UNIVERSITIES TARGETED BY INCREASING PHISHING & RANSOMWARE ATTACKS
Sept 2017

@drjessicabarker
Awareness ≠ Behaviour

Educause 2018
Harnessing Human Bias

Educause 2018
Ctrl  Alt  Del

Educause 2018
PRIVACY AND SECURITY

The Number of People Who Fall for Phishing Emails Is Staggering

Educause 2018

35% of Users Have Weak Passwords; the Other 65% can Be Cracked

Preempt

Password leaks from public breaches help us learn how people think, allowing us to identify patterns and build dictionaries of passwords. As password cracking methods evolve, uppercase characters, common characters, special characters (e.g., *#%^), and numbers are not random enough longer passwords are needed.

People reuse passwords. They create them, add digits to them, and even use identical or similar passwords with others. As data scientists, it is our

Security

NIST: People have given up on cybersecurity – it's too much hassle

Fine, go ahead, cyber-crowd - cyber-steal my muffin cyber-recipe

Thomas Claburn in San Francisco 8 Oct 2018 18:10:28

Humans are (still) the weakest cybersecurity link

Companies are regularly compromised by social engineering schemes, such as phishing and ransomware. Here's what they can do prevent attacks and, if that's too late, mitigate the damage.

Worst, most common passwords for the last 5 years

Here are the worst and most common passwords for the last five years as compiled by Splashdata.
Lesson 1
Get Social Proof on Side

Educause 2018
FULL
EMPTY
Educause 2018
OPTIMISM IS MORE POWERFUL THAN FACTS
Optimism makes people try harder.
Lesson 2
Engage with Optimism
1. Appraise threat

Appraise efficacy

2. susceptibility → motivation

Perceived efficacy

Control danger or fear

@drjessicabarker

Educause 2018
Educause 2018
Educause 2018
“We need to overcome our habit of trying to scare people into action, and instead highlight the rewards that come with reaching our goals”

Tali Sharot, The Optimism Bias
Lesson 3
Spread Hope Not Fear
Educause 2018
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1 = 1</td>
<td>2 = 2</td>
<td>3 = 3</td>
<td>4 = 4</td>
</tr>
<tr>
<td>2</td>
<td>2 = 2</td>
<td>4 = 4</td>
<td>6 = 6</td>
<td>8 = 8</td>
</tr>
<tr>
<td>3</td>
<td>3 = 3</td>
<td>6 = 6</td>
<td>9 = 9</td>
<td>12 = 12</td>
</tr>
<tr>
<td>4</td>
<td>4 = 4</td>
<td>8 = 8</td>
<td>12 = 12</td>
<td>16 = 16</td>
</tr>
<tr>
<td>5</td>
<td>5 = 5</td>
<td>10 = 10</td>
<td>15 = 15</td>
<td>20 = 20</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>6 = 6</td>
<td>12 = 12</td>
<td>18 = 18</td>
<td>24 = 24</td>
</tr>
<tr>
<td>7</td>
<td>7 = 7</td>
<td>14 = 14</td>
<td>21 = 21</td>
<td>28 = 28</td>
</tr>
<tr>
<td>8</td>
<td>8 = 8</td>
<td>16 = 16</td>
<td>24 = 24</td>
<td>32 = 32</td>
</tr>
<tr>
<td>9</td>
<td>9 = 9</td>
<td>18 = 18</td>
<td>27 = 27</td>
<td>36 = 36</td>
</tr>
<tr>
<td>10</td>
<td>10 = 10</td>
<td>20 = 20</td>
<td>30 = 30</td>
<td>40 = 40</td>
</tr>
</tbody>
</table>
Stereotype Threat & Women’s Math Performance
HUMANS – THE WEAKEST LINK IN CYBER-SECURITY

Cybersecurity’s Weakest Link: Humans

The Weakest Link in the Cyber-Security Battle: The Human Factor
22 Mar, 2017

Cybersecurity is only as strong as your weakest link—your employees

The Human ‘Attack Surface’ May Be Your Weakest Link

The Weakest Link in the Cybersecurity Chain Is Sitting at the Keyboard

THE WEAKEST LINK IN YOUR CYBER RESILIENCE STRATEGY MIGHT BE YOUR PEOPLE

Cyber Risk: People Are Often The Weakest Link In The Security Chain

You Are the Weakest Link: 5 of the Biggest Cyber Security Risks for Businesses

Incoming: The Weakest Link in Security Chain Is People, Not Technology

The Weakest Link In Cybersecurity Systems? You And Me

@drjessicabarker
“Users are stupid”
If security doesn’t work for people, it doesn’t work

Emma W
People-Centred Security lead
NCSC

Educause 2018
Lesson 4
Resist Stereotypes

Educause 2018
Self-Efficacy in Information Security
Rhee, S-K et al (2009)

Individuals with high SEIS:

- used **more security software and features**
- applied **security updates/patches**
- Had better **security care behaviour**
Lesson 5
Raise Self-Efficacy

Educause 2018
<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description of an effective frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Do not exacerbate Cybersecurity</td>
<td>Put the need in a realistic perspective. Exaggeration will only exacerbate the problem and work against the objective in the long term.</td>
</tr>
<tr>
<td>2) Make it clear who the villains are</td>
<td>Villains should be clearly recognizable as evil.</td>
</tr>
<tr>
<td>3) Give cybersecurity a face by putting the heroes in the spotlight</td>
<td>Those who are guarding and protecting society should be placed in the forefront. Demonstrate their successes.</td>
</tr>
<tr>
<td>4) Show its importance for society</td>
<td>The benefits of taking action should be emphasized. Cybersecurity is key to economic growth and the prosperity of nations.</td>
</tr>
<tr>
<td>5) Personalize for easy recognition by the public</td>
<td>Connect cybersecurity to the daily life of people to ensure easy recognition. Groups are different.</td>
</tr>
<tr>
<td>6) Connect to undcurrent issues</td>
<td>Cybersecurity is closely interwoven with other issues that do receive political attention.</td>
</tr>
</tbody>
</table>

*Building Cybersecurity Awareness: The need for evidence-based framing strategies*

*Hans de Bruijn and Marijn Janssen, 2017*
Password security

Attacks use a variety of techniques to discover passwords, including using powerful tools freely available on the Internet. The following advice makes password security easier for your users - improving your system security as a result.

How passwords are cracked...

Interception
Passwords can be intercepted as they are transmitted over a network.

Brute Force
Automated guessing of billions of passwords until the correct one is found.

Searching
IT infrastructure can be searched for electronically stored password information.

Stealing Passwords
Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing
Personal information, such as name and date of birth, can be used to guess common passwords.

Shoulder Surfing
Observing someone typing their password.

Social Engineering
Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging
An installed keylogger intercepts passwords as they are typed.

...and how to improve your system security

Help users cope with ‘password overload’
- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of multiple unsuccessful login attempts.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords
- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength algorithms.

For more information go to: www.ncsc.gov.uk  @ncsc

Educause 2018
Phishing attacks: Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

**Layer 1**
Make it difficult for attackers to reach users.
- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same.
- Filter or block incoming phishing emails.

**Layer 2**
Help users identify and report suspected phishing emails.
- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

**Layer 3**
Protect your organisation from the effects of undetected phishing emails.
- Protect your account: make authentication more resistant to phishing (such as setting up 2FA) and ensure authorisation only gives privileges to people who need them.
- Protect your users from malicious websites by using a proxy server and an up-to-date browser.
- Protect your devices from malware.

**Layer 4**
Respond quickly to incidents.
- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.
1. Get social proof on side
2. Harness optimism
3. Spread hope not fear
4. Resist stereotypes
5. Raise self-efficacy
References


Oliveira, D et al (2008) 'It’s the Psychology Stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer’s blind spots’ ACSAC pp. 296-205


Recommended Reading

THINKING, FAST AND SLOW
DANIEL KAHNEMAN

NEW INTERNATIONAL EDITION

nudge

‘Hot stuff’
SUNDAY TIMES

‘Hugely influential’
GUARDIAN

Improving decisions about health, wealth and happiness

THALER & SUNSTEIN

THE INFLUENTIAL MIND
TALI SHAROT
Author of The Optimism Bias

Educause 2018