# Human Issues in Cybersecurity

## Challenging Faulty Assumptions and Cognitive Biases

**Troy Berg**
Chair and Professor
Infrastructure and Computing Technology Department
Okanagan COLLEGE

# Everyone, meet Becky

## Becky Thurmanson

- Age: 32
- Employer: Align Chiropractic Inc.
- Occupation: Payroll Clerk
- Time with Company: 7 years

- Head of the staff social committee
- Remembers everyone’s birthday
- Brings muffins for the staff room at least once per month

# Everyone, meet Becky

## Becky Thurmanson

- Age: 32
- Employer: Align Chiropractic Inc.
- Occupation: Payroll Clerk
- Time with Company: 7 years

- Head of the staff social committee
- Remembers everyone’s birthday
- Brings muffins for the staff room at least once per month
- Workstation Password: Kitten2023

' UPS® ' <Noreply-cc5Tb0Xg@cc5Tb0Xgcc5Tb0Xg.ca>
To [redacted]

Reply | Reply All | Forward | ...
None

If there are problems with how this message is displayed, click here to view it in a web browser.

# UPS

## INTERNATIONAL SHIPPING AND LOGISSICS SERVICE |UPS CANADA

You have **(1) package waiting for delivery.**
Use **your code to track it and receive it**

### Dear Customer

Schedule your delivery and subscribe to our calendar notifications to avoid this from happening again!

**Your Tracking Code:** 29194773

Receive Your Package


Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 13 hours 43 minutes 10 seconds
Start the decryption process

# Human Issues in Cybersecurity

## Challenging Faulty Assumptions and Cognitive Biases

**Troy Berg**
Chair and Professor
Infrastructure and Computing Technology
Okanagan College

# Faulty Assumption #1

**Humans will behave rationally, so blame the user!**

# Faulty Assumption #1 – True Story


- In 2021, an executive publicly blamed an intern for choosing a weak password.
- The subsequent lawsuit said SolarWinds used an easily guessable password “solarwinds123” on an update server, which was subsequently breached by hackers “likely Russian in origin.”

Chandu Gopalakrishnan. https://techcrunch.com/2021/03/13/why-blaming-the-intern-wont-save-startups-from-cybersecurity-liability/

# Faulty Assumption #1 – Counter Approach

- Understand and acknowledge that humans are complex.
- Never assume that people will know or make the best choice.
- “Blame” is a matter of context, and assigning blame rarely helps achieve cybersecurity goals.

# Faulty Assumption #1 – Counter Approach

**Revised Cybersecurity Mantra:**

**We will not *automatically* blame the user.**

# Faulty Assumption #2

**The primary goal of cybersecurity is security.**

# Faulty Assumption #2 – True Story

- In 2019, researchers examined the relationship between data breach remediation and hospital care quality.
- Following the breach, new cybersecurity measures slowed the ability to access health records and to order, review, and execute tests in the emergency room.
- The longer the wait, the higher the mortality rate.

Choi, Sung J., Johnson, M. Eric, and Lehmann, Christopher U., “Data Breach Remediation Efforts and Their Implications for Hospital Quality,” Health Services Research, Vol. 54, No. 5 (2019): 971–980. https://doi.org/10.1111/1475-6773.13203

# Faulty Assumption #2 – Counter Thought

- Cybersecurity is not the primary goal – the goal of cybersecurity is to maximize and support what the user or organization is trying to accomplish.
- Organizations have goals that can be *enabled* and *protected* by security, but the primary tasks matter most.

# Faulty Assumption #2 – Counter Thought

**Revised Cybersecurity Mantra:**

**As cybersecurity professionals, we are here to help organizations achieve their goals with an *appropriate* amount of security.**

# Faulty Assumption #3

**Cybersecurity education needs to be scary to be effective.**

# Faulty Assumption #3 – True Story

- **Researchers in the UK have correlated calculable losses of productivity within organizations due to fear-based approaches to cybersecurity.**
- **Fearmongering in cybersecurity costs your organization time, productivity and money, and has a direct negative impact on organizational culture.**

Palmer, Danny. “Don’t let cybersecurity be driven by fear, warns NCSC chief.” https://www.zdnet.com/article/dont-let-cyber-security-be-driven-by-fear-warns-ncsc-chief/

# Faulty Assumption #3 – Counter Thought

- Instead of fear, consider focusing on messages and campaigns that encourage strength and stability, promote innovation and creativity, and empower users.
- Instead of threatening, be pragmatic.
- Users can be allies in your cybersecurity fights rather than be treated as the problem.

# Faulty Assumption #3 – Counter Thought

**Revised Cybersecurity Mantra:**

**We will recognize that fearmongering and "blame-and-shame" approaches to cybersecurity can be counterproductive to the goals and culture of my organization.**

# Faulty Assumption #4

**Cybersecurity is about obvious risks.**

# Faulty Assumption #4 – True Story

- When asked what are the most common risks we should be concerned about, most cybersecurity professionals cite the obvious ones.
  - Social engineering/phishing
  - Identity-related breach / password compromise
  - Ransomware
  - Denial of Service

# Faulty Assumption #4 – Counter Thought

- Our cybersecurity thinking must go well beyond the obvious.
- Do we have adequate controls to govern and monitor our policies and procedures?
- How are we dealing with insider threats?
- What about user training and mentorship?
- How about administrator fatigue?

# Faulty Assumption #4 – Counter Thought

**Revised Cybersecurity Mantra:**

**Yes, cybersecurity has obvious risks, but as a cybersecurity professionals, we will train ourselves to look and plan for things that are beyond the obvious.**

# Cognitive Bias #1

## Choice Affirmation Bias

- Occurs when we have previously made some choice, and the current situation relates to that choice.
- Rather than make a (correct) decision that casts our previous choice in a negative light, we make additional incorrect decisions.

# Cognitive Bias #1

## Example

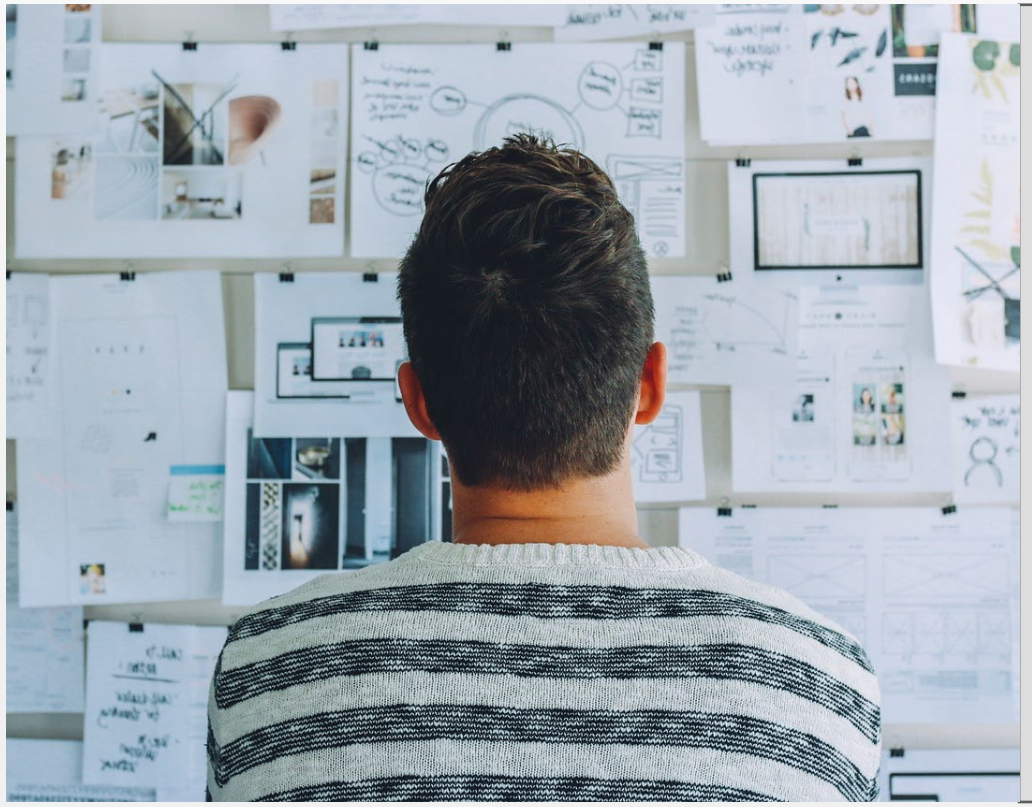
- For example, a high-level IT manager championed the decision to invest heavily in the acquisition of a particular security monitoring software.
- A colleague is concerned that the solution does not seem fully effective and wants to license another solution to run alongside the first.
- The manager vetoes the suggestion because he won’t permit any criticism of his first decision, even if the evidence presented is to the contrary.

# Cognitive Bias #1 – Counter Thought

**Revised Cybersecurity Mantra:**

**As a cybersecurity professionals, we will train ourselves to be open-minded, humble and flexible enough to rethink our own decisions when presented with new information.**

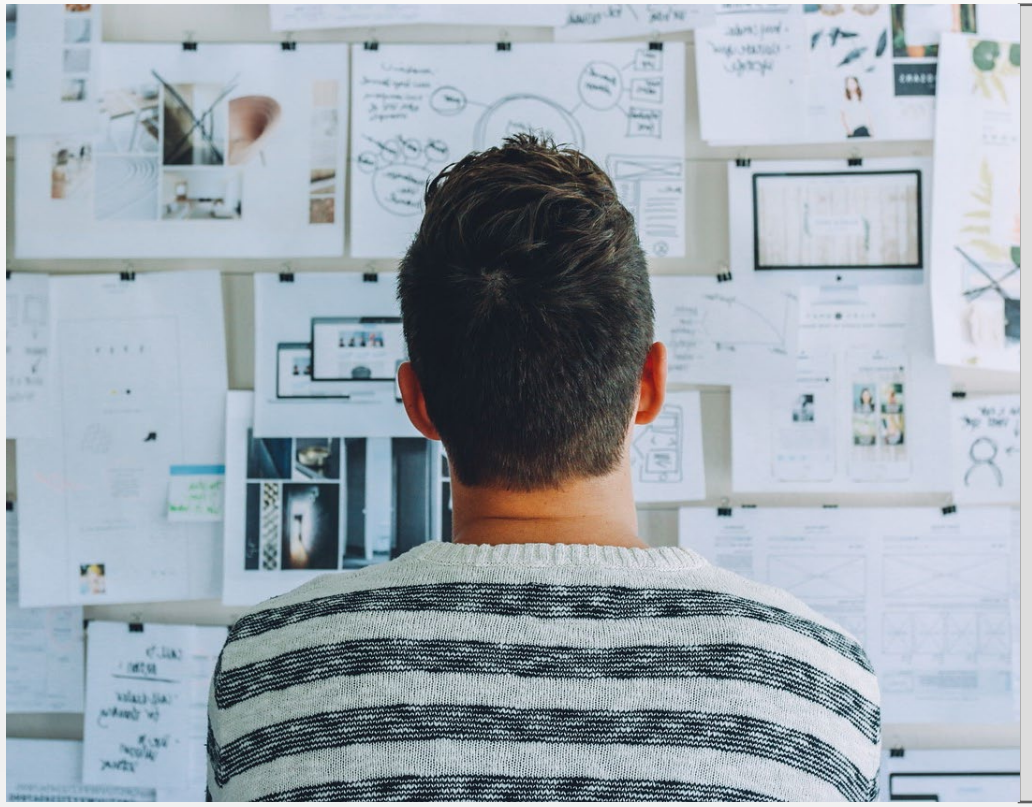
# Cognitive Bias #2



## Hindsight Bias

- Occurs when, after an incident, we think that we would have seen the cues or event that led up to the problem, so the person who did not see them is the person to blame.

# Cognitive Bias #2 – Counter Thought



**Revised Cybersecurity Mantra:**

**As cybersecurity professionals, rather than blaming people and telling everyone how we would have "saved the day," we will take the information we've learned and use it constructively to hopefully prevent the event from happening again.**

# Cognitive Bias #3

## Social Proof Bias

- Sometimes also known as the bandwagon effect or conformity bias
- Occurs when someone, when confronted with a new or uncertain situation, we look to what others are doing and copy that behavior

# Cognitive Bias #3 – Counter Thought

**Revised Cybersecurity Mantra:**

**As cybersecurity professionals, we will recognize that social proof can be useful, but also a pitfall.**

**Instead of going with the crowd, we'll make well-researched, carefully reasoned decisions based on the needs of our own environment.**

# Cognitive Bias #4


## Hasty Generalization

- The problem must have been the user.
- An administrator must have made an error.
- The attack must have begun with extensive reconnaissance.

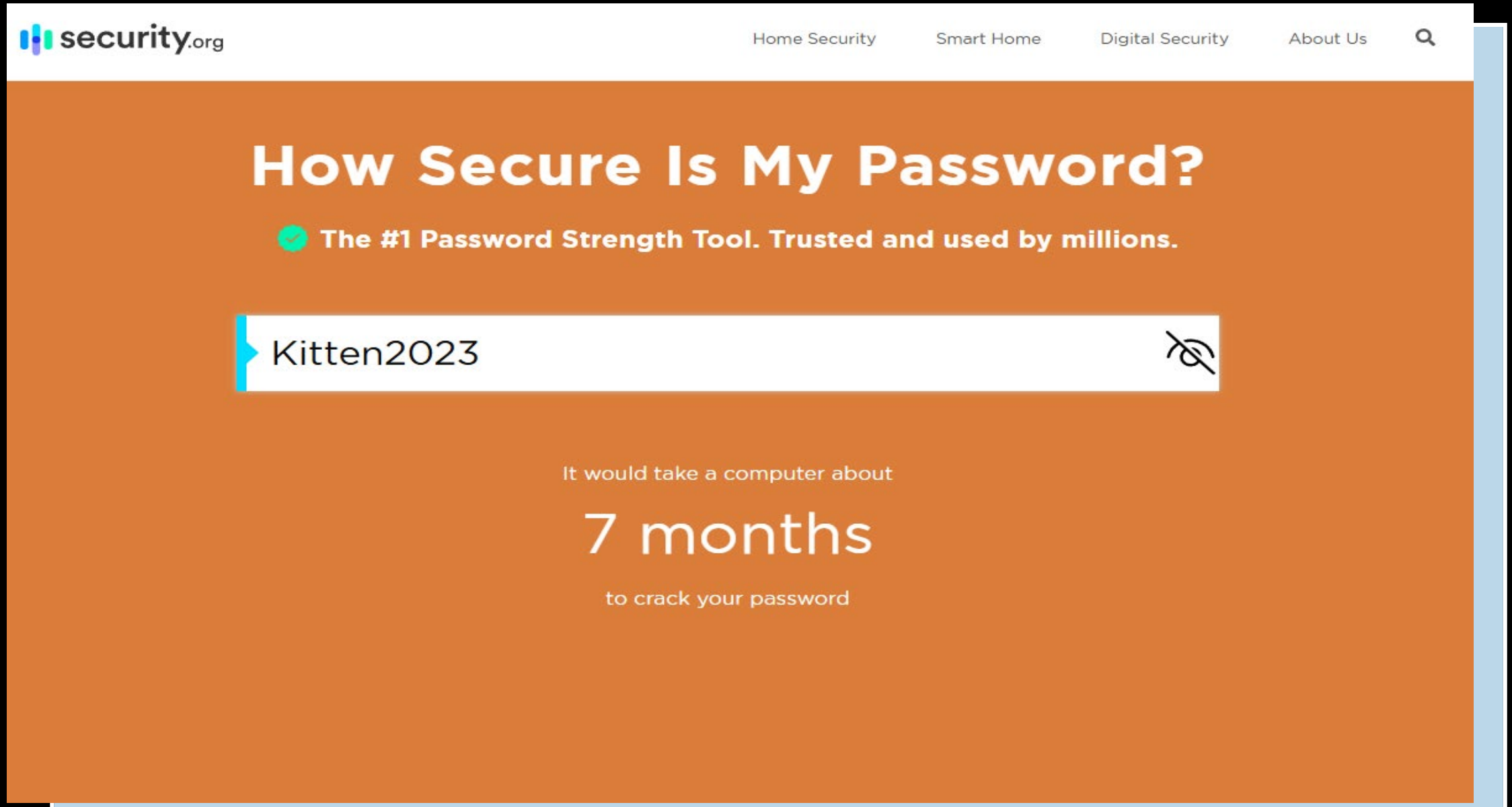
# Cognitive Bias #3 – Counter Thought


**Revised Cybersecurity Mantra:**

**As cybersecurity professionals, we will recognize that quick generalizations are often misguided.**

# In summary…


- Cybersecurity is an evolving discipline. Be open to new perspectives.
- There's a vital distinction between being uninformed and misinformed.
- Mindsets can be pervasive – challenge them.
- Fallacies, assumptions, and biases are ever-present in our work.
- Whenever possible, choose to be effective, informed, and reasonable.


security.org
Home Security
Smart Home
Digital Security
About Us
How Secure Is My Password?
The #1 Password Strength Tool. Trusted and used by millions.
Kitten2023
It would take a computer about
7 months
to crack your password