September 29, 2020

Security Awareness Month Workshop

Cybersecurity: Before, During, and After COVID-19

Russ Mumford

Visible Statement®

Security Remembered.
Awareness Delivered

A product of Greenidea®

Hello to All

I'm Russ Mumford, Founder and CEO of Visible Statement®.

I'm here to talk with you for a few minutes about how Covid-19 has impacted security awareness.

I have a personal approach to this issue...

First, you need to get the attention of your audience.

Let's see if this gets your attention...

I thought it might.

Now let's begin by discussing one of the most important factors in cybersecurity:

Human Error

Human Error

An astonishing 95 percent of all security incidents involve human error.

Cybersecurity experts, including the FBI and cybersecurity professionals from around the world, confirm the biggest weakness in cyber-security is human error, from following links to phishing scams to visiting bad websites, enabling viruses and falling victim to other advanced persistent threats.

Huffington Post, 05/10/2017

Here's a trick question.

(We all know the answer to this one….)

QUESTION:

What are the three most important factors in Real Estate?

ANSWER:

LOCATION
LOCATION
LOCATION

One final question…

QUESTION:

What are the three most important factors in Security Awareness?

ANSWER:

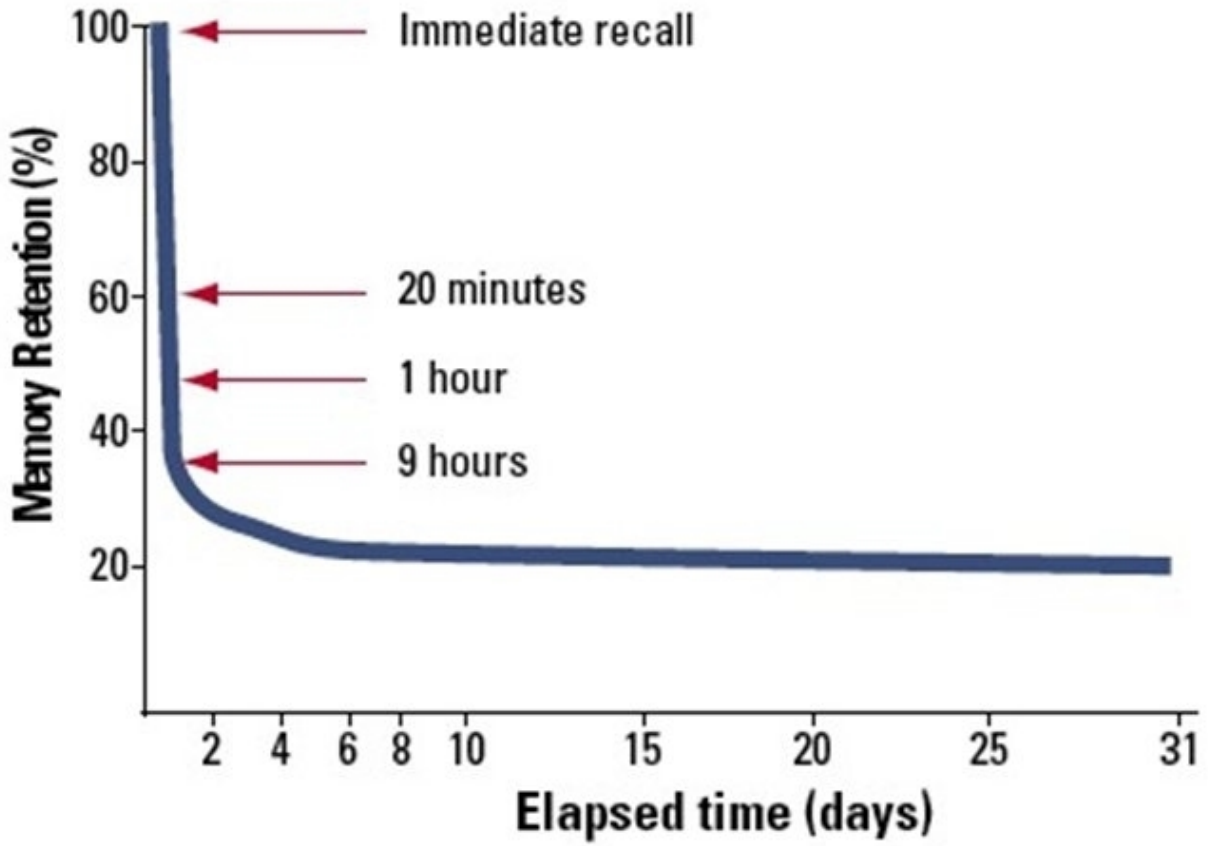
REPETITION
REPETITION
REPETITION

Why is that?

The Ebbinghouse "Forgetting Curve"

Originally published in 1885, it is as relevant today as it was then.

80% **of what's taught is FORGOTTEN within *days*.**



Fortunately,
there's Good News.

Retention is as Easy
as 1, 2, 3. (almost)

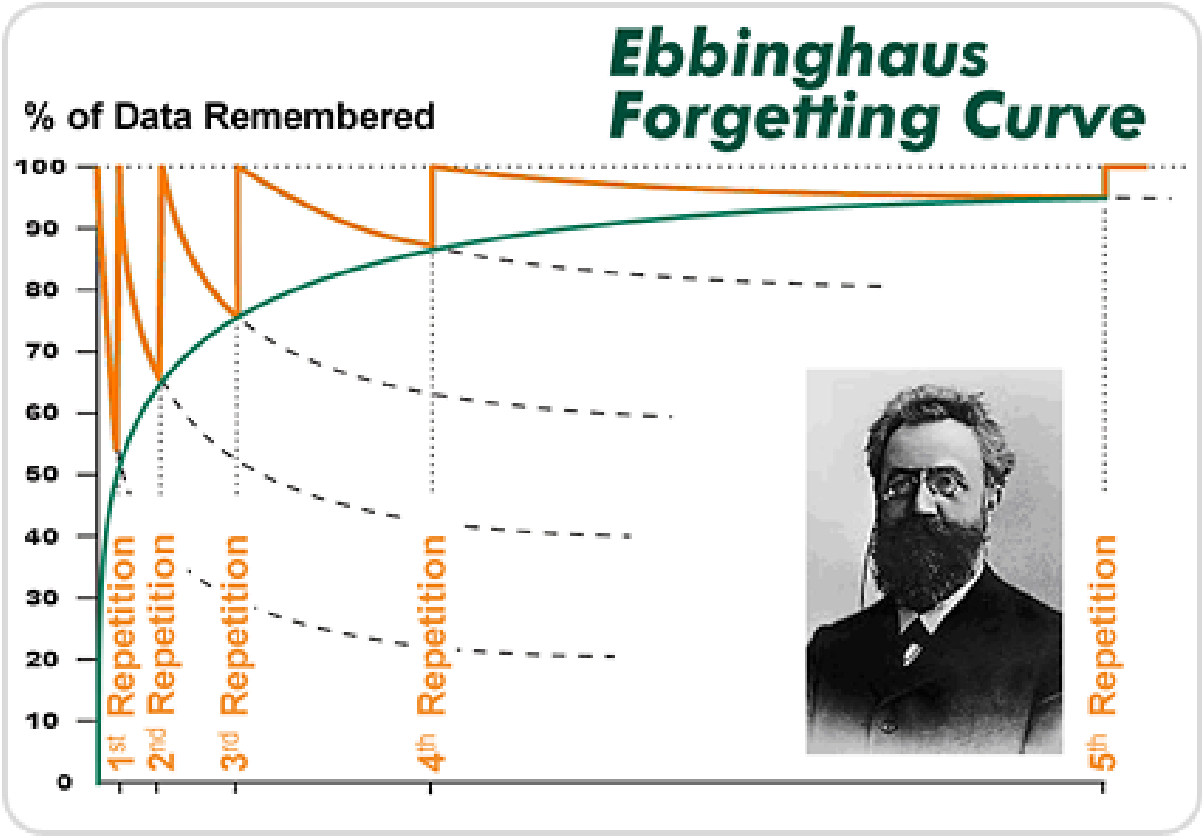
Actually…it's as easy as

1, 2, 3, 4, 5, 6

Here's how.

Repetition, Repetition, Repetition

With several spaced Repetitions, Retention climbs from near *zero* to *90%.* – an amazing transformation!



Cybersecurity:
Before, During, and After

COVID-19

Before The Pandemic

Before The Pandemic

Prior to the pandemic, corporations consisted mainly of employees working in-house (offices), where their companies had control over managed services and networks, and the ability to monitor incidents, etc.

Frequently one desktop standard in a controlled environment, therefore more ability to influence behavior.

During The Pandemic

During The Pandemic

COVID-19 is an emerging, rapidly evolving situation, affecting different organizations in different ways.

Priorities:

During The Pandemic

COVID-19 is an emerging, rapidly evolving situation, affecting different organizations in different ways.

Priorities:

1. Securing work-from-home arrangements on an unprecedented scale now that organizations have told employees to stop traveling and gathering,

During The Pandemic

COVID-19 is an emerging, rapidly evolving situation, affecting different organizations in different ways.

Priorities:

1. Securing work-from-home arrangements on an unprecedented scale now that organizations have told employees to stop traveling and gathering,
2. Maintaining the confidentiality, integrity, and availability of consumer-facing network traffic as volumes spike—partly as a result of the additional time people are spending at home.

The types of attacks companies are experiencing During COVID-19

Corporate Attacks

- **Phishing and Malspam** – Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.

Corporate Attacks

- **Phishing and Malspam** – Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.
- **Credential Stuffing** –multi-factor authentication (MFA). Along with securing accounts with MFA.

Corporate Attacks

- **Phishing and Malspam** – Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.
- **Credential Stuffing** –multi-factor authentication (MFA). Along with securing accounts with MFA.
- **Ransomware** – In some cases it is possible malspam emails that start a ransomware infection will use a COVID-19 lure.

Corporate Attacks

- **Phishing and Malspam** – Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.
- **Credential Stuffing** –multi-factor authentication (MFA). Along with securing accounts with MFA.
- **Ransomware** – In some cases it is possible malspam emails that start a ransomware infection will use a COVID-19 lure.
- **Remote Desktop Protocol (RDP) Targeting** – An increase in the number of employees connecting remotely means an increase in the number of systems with open RDP (port 3389) potentially being scanned.

Corporate Attacks

- **Phishing and Malspam** – Remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization. They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments.
- **Credential Stuffing** –multi-factor authentication (MFA). Along with securing accounts with MFA.
- **Ransomware** – In some cases it is possible malspam emails that start a ransomware infection will use a COVID-19 lure.
- **Remote Desktop Protocol (RDP) Targeting** – An increase in the number of employees connecting remotely means an increase in the number of systems with open RDP (port 3389) potentially being scanned.
- **Distributed Denial of Service (DDoS) Attacks** – Downtime from an attack is even more detrimental with a remote workforce. A larger remote workforce can even act as an unintentional DDoS attack, simply because more users are trying to access services at the same time.

After the Pandemic

Predictions for a Post-COVID-19 Workplace

McKinsey & Company Sept 28, 2020

After The Pandemic

Cybersecurity post-COVID-19

1. 85% of companies accelerated digitization.

After The Pandemic

Cybersecurity post-COVID-19

1. 85% of companies accelerated digitization.

2. 67% accelerated automation and artificial intelligence during the pandemic, with faster expansions in firms that had a greater shift to remote work, especially the financial services and tech sectors.

After The Pandemic

Cybersecurity post-COVID-19

1. 85% of companies accelerated digitization.

2. 67% accelerated automation and artificial intelligence during the pandemic, with faster expansions in firms that had a greater shift to remote work, especially the financial services and tech sectors.

3. McKinsey's survey suggests the mix of jobs available post-pandemic will be different, *predicting increased demand for contractors, gig workers and hygiene, cybersecurity and data analytics jobs.*

Securing Employee Home Networks

Patching – Patching systems to remedy known vulnerabilities

Home Computers – Recommend employees implement security on these devices

Printers – Employees should look up printer security

USB Devices –Staff should use only company-approved USB devices.

Storage – Designate how and where an employee can store sensitive information.

Access by Others – Ask employees to keep work devices for professional use only.

Secure Video Conferencing – Keeping meetings private and password-protected.

Once again…

QUESTION:

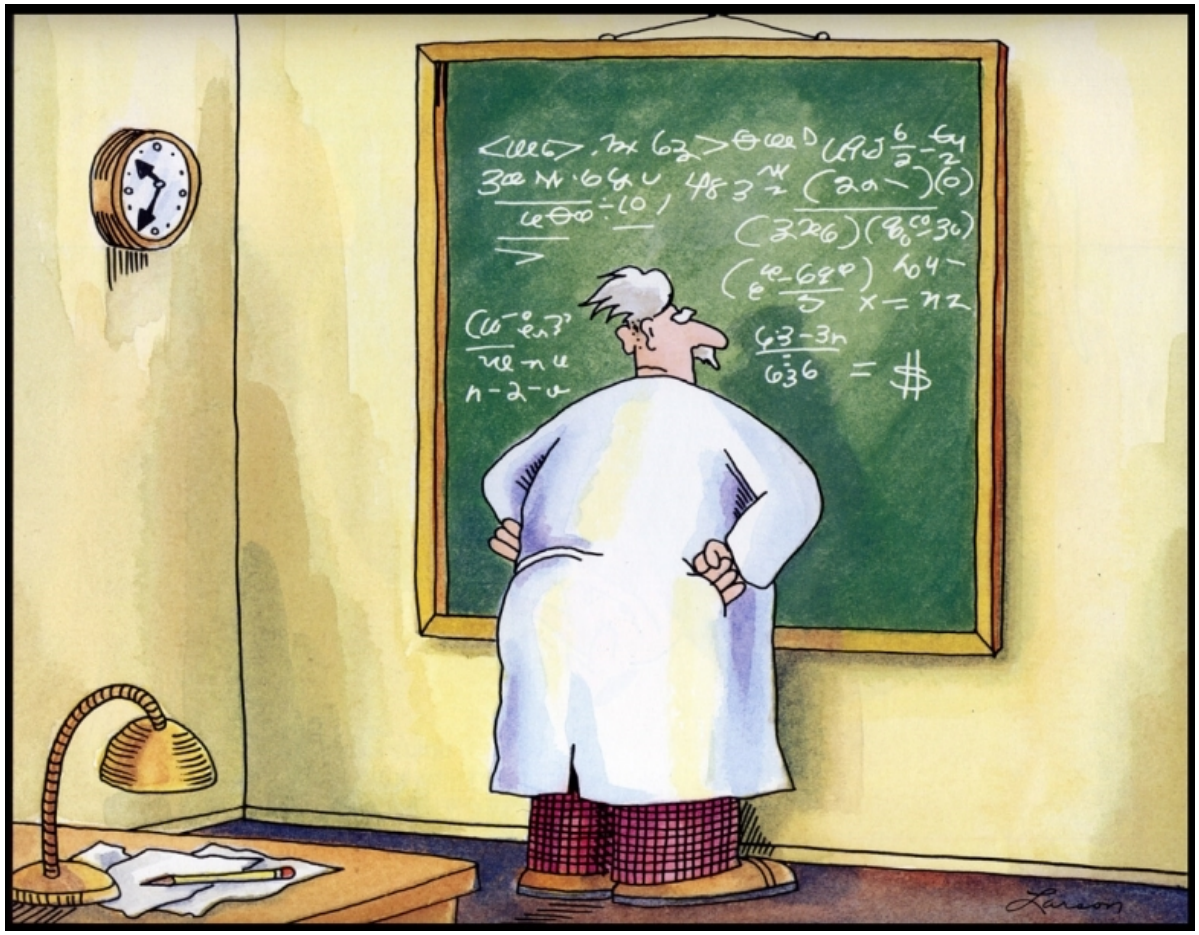
What are the three most important factors in Security Awareness?

ANSWER:

REPETITION
REPETITION
REPETITION

Thank You For Your Time!

For we all know, as Einstein discovered years ago…



Time is Money!

Stay Well.
Stay Safe.
Stay Aware.

Russ Mumford
Visible Statement®
Security Remembered
Awareness Delivered