



Because learning changes everything.®

# Cybersecurity in a Pandemic – A Guide for Educators

With Casey Wilhelm and Ted  
Tedmon

---

Hosted by Dean Karampelas  
McGraw-Hill Education



# Cybersecurity and COVID-19 – The Risks

- **Security Risks From Increased Remote Working and Learning**
- **Overwhelmed Cybersecurity Teams**
- **Disenfranchised Unemployed Workers**



**Google Reports a 350% increase in Phishing Attacks Over 18 Million Attacks Per Week in April**

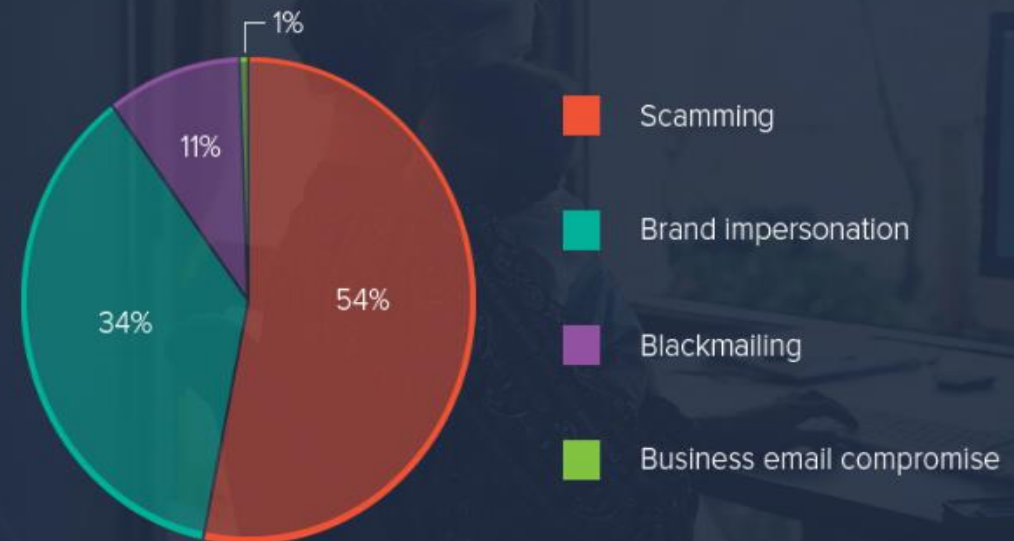
# Spear-Phishing Attacks on the Rise

Past 3 month IOCs show dramatic increases in:

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution, using coronavirus- or COVID-19-themed lures
- Registration of new domain names containing wording related to coronavirus or COVID-19
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure

<https://www.us-cert.gov/ncas/alerts/aa20-099a>

## Types of coronavirus-related spear-phishing attacks

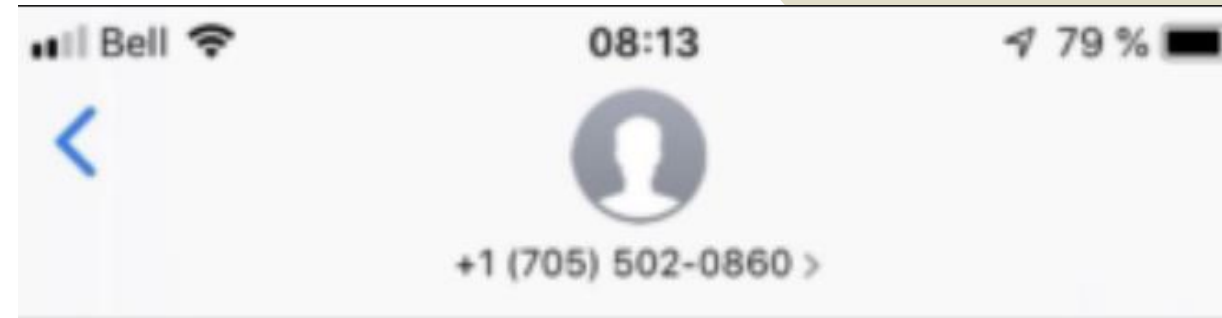


**Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020**

# Mobile Risks - COVID-19

- Apple, Google, and Microsoft developing RPID Technology
- Phone Scams – Primarily Government Impersonation Fraud
- Dramatic Increase in Smishing Attacks

[US-Cert/APWG https://apwg.org/](https://apwg.org/)



Message  
Aujourd'hui 02:49

Due to the recent shortage of face masks, the Red-Cross will be distributing one free box per household. Visit <http://RedCross-mask.ca> to get one.

**COVID-19 smishing attacks include malicious links that claim to provide information about the virus, free masks or stimulus payments.**



# COVID-19 What Students Need From Their Professors Right Now

- **Trust**
- **Compassion**
- **Stability**
- **Hope**



**In an Uncertain World, Professors Can Provide Students with Needed Perspective**

# What Professors Should Know About Their Students

- **43% Experience Significant Anxiety and Nervousness**
- **40% - Change in Work Routine had a Negative Impact on Classwork**
- **38% - Had to Abruptly Change Their Housing Situation**

<https://www.ncbi.nlm.nih.gov/2020/vol20>



**Professors should show a clear way forward. Students are amazingly resilient. There is an observed “Rally Effect.”**

# Tip #1: Focus Assignments On Current Events

- **Cases from today's news stories**
  - Biggest Hacks of 2020
  - Latest Ransomware attacks
- **Discussions**
  - What impact has COVID-19 had on our dependence on vulnerable systems?
  - Is Zoombombing a new phenomenon?
- **Writing prompts**
  - What risks may arise as workers return to work and students return to school



**Keep the topics relevant to increase engagement!**

# Tip #2: Keep it Interactive

- **Maintain Busy Office Hours**
  - Double your availability – You’ve probably got a shorter commute!
- **Create Sign-up Space**
  - It’s easier to get students to commit to a time in the future
- **Mandate Student Visits**
  - Require an early meeting to ease anxiety



**Try to Build a Personal Relationship with as Many Students as Possible**



# Tip #3: Keep Online Classes Fun

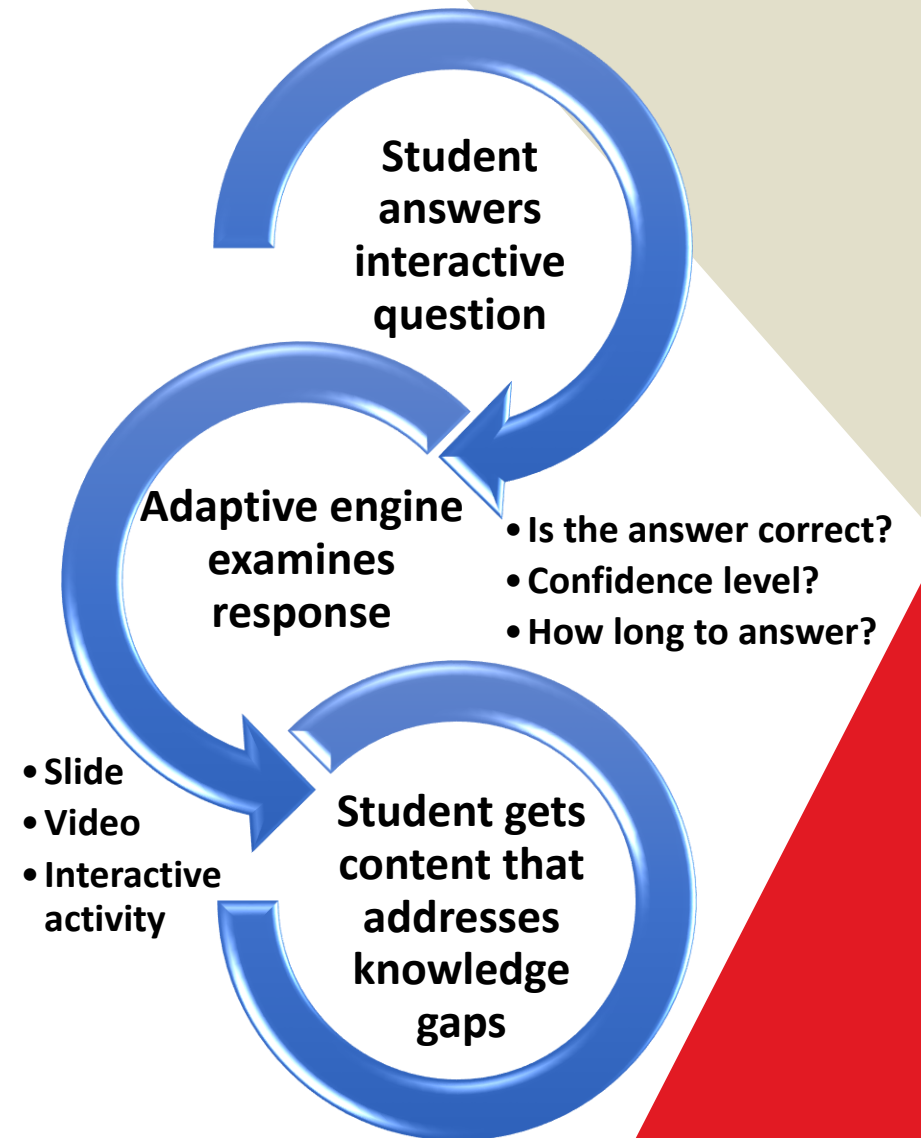
- **Minimize PowerPoint Time**
- **Use Frequent Cognitive Switching**
- **Use More Activities to Keep Students Engaged**
- **Limit Each Student's Time for Input (and yours!)**

**Smile Often – It's Contagious!**



# Use Adaptive Learning

- **Students have diverse knowledge backgrounds**
- **Adaptive learning teaches to knowledge gaps**
- **Keeps well-prepared students engaged without intimidating those with less knowledge**



## Adaptive Learning Returns Control to Students

# Remember that Students Learn Differently

## **Millennials (ages 23-39)**

- **Believe they can multitask – Cognitive task switching is the norm**
- **Challenge Authority – Speak their minds**
- **Crave Recognition – Demand feedback and praise**
- **Short Attention Spans – Organization challenges**

## **Gen Zs (ages 15-25)**

- **Social – Flipped educational approach. Facilitating rather than lecturing**
- **Digital – Digital natives, but often lack keyboarding skills**
- **Visual – Expect video and images**
- **Non-Linear learners – Comfortable jumping between concepts**

# Establish a Predictable Cadence for Assignments

- **Multiple weekly due dates**
- **Award points for all assignments**
- **Use formative assessments**



**Redundancy Builds Retention**



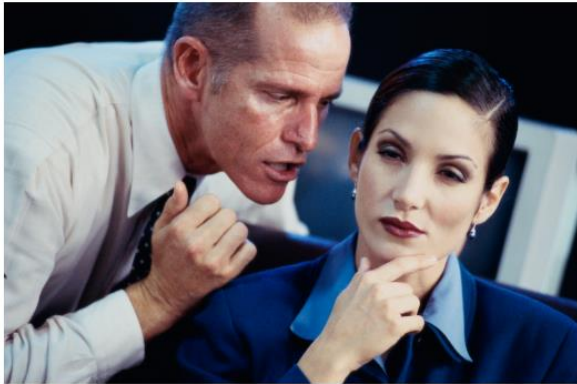
# Use Curiosity and Competition

- **Encourage feedback that promotes critical thinking**
- **Use individually-performed group exercises**
- **Apply concepts – Do more, lecture less**



**Remember - Millennials Want to Be Heard**

# Connect Master 2.0 – Multiple Learning Styles



## Question Multiple Choice

The cybersecurity term "social engineering" is best defined as \_\_\_\_\_.

- the act of manipulating or tricking people into sharing their confidential, personal information
- the impersonation of known, trusted entities to deceive people into making payments
- the use of online survey or poll results to gauge public sentiment and influence public opinion
- the creation of social media posts designed to spread and bolster false information

Rate your confidence to submit your answer

High

Medium

Low

## Social Engineering

**Social engineering** is the manipulation of people so that they give up their confidential information.

Social engineering is designed to get individuals to give criminals many types of sensitive information, including:

- Passwords
- Bank information
- Access to computers or networks
- Social Security numbers

Social engineering attacks exploit individuals' trust and lack of knowledge about what types of information should be divulged.



Social engineering attacks prey on people's trust to procure sensitive information

- **Accessible**
- **Chunking Design**
- **Images Encourage Learning**

# Connect Master 2.0 – Multiple Learning Styles

## Cybersecurity Threats, Vulnerabilities, and Exploits

### Cybersecurity Threats

According to the National Institute of Standards and Technology (NIST), a **cybersecurity threat** is an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

Assets include information, software, and hardware. The specific causes of asset loss arise from a variety of situations and events related to adversity, which are typically referred to as disruptions, hazards, or threats. Asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions.

Cybersecurity threats should be assessed and remediated in order to prevent ongoing or future impacts.

### Cybersecurity Vulnerabilities

**Cybersecurity vulnerabilities** are weaknesses or flaws in system security procedures, design, implementation, and control that could be compromised accidentally or intentionally.

System compromises can result in security breaches, lost information or data, system outages, and violations of an organization's system security policy.



## Review: Cybersecurity Threats, Vulnerabilities, and Exploits

 **CLICK AND LEARN: Cybersecurity Threats, Vulnerabilities, and Exploits**

### What is a cybersecurity threat?

A cybersecurity threat is an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

### What is a cybersecurity vulnerability?

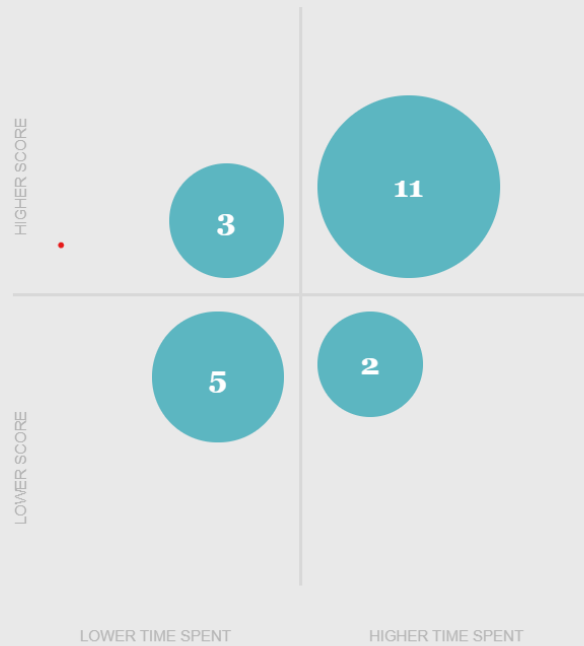
A cybersecurity vulnerability is a weakness or flaw in system security procedures, design, implementation, and control that could be compromised accidentally or intentionally.

### What is a cybersecurity exploit?

An cybersecurity exploit is the means through which a system vulnerability can be used by a hacker to execute a malicious activity on a system.

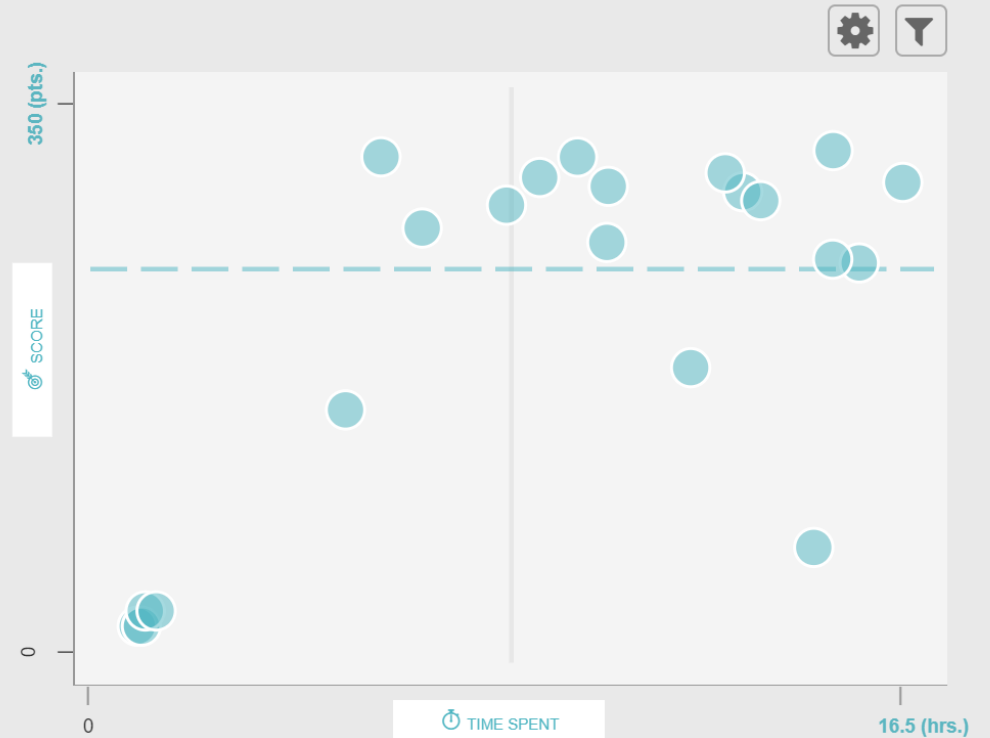
# Connect Master 2.0 – Powerful Analytics

## How is my section doing?



Student Distribution - at a glance | 21 / 21 Students [Dive Deeper](#)

## How are my students doing?







Because learning changes everything.®

Thank You!



---

@ Dean.Karampelas@mheducation.com  
630-716-0232  
www.mheducation.com



---

Casey Wilhelm  
@ crwilhelm@nic.edu  
208-769-3262



---

Ted Tedmon  
@ rstedmon@nic.edu  
208-769-3260

