

**CARBONITE**<sup>®</sup>  
an **opentext** company

**WEBROOT**<sup>®</sup>  
an **opentext** company

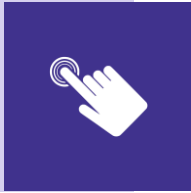
# Phishing: Don't Take the Bait

November 12<sup>th</sup>, 2020 | Phil Karcher, Principal Product Manager, Security Awareness Training

# The Growing Problem of Phishing



**1 in 3** have **clicked on a phishing email** in the last year in the U.S.



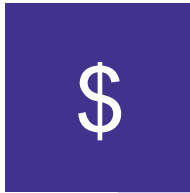
**#1 threat action variety** in data breaches

Every day, **2%** of users will click on a phishing link



**76%** of users **will click on an email** without knowing the sender

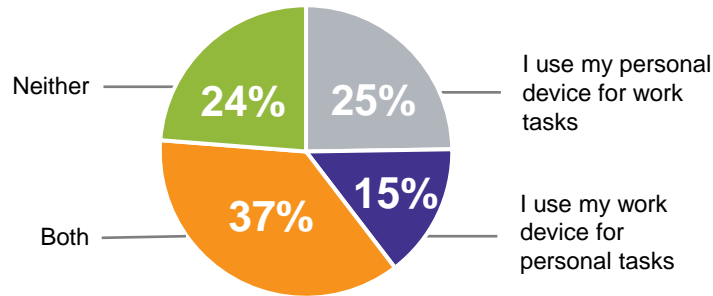
**67%** of orgs are concerned about phishing as the primary attack vector



**CC: \$12-35, ATM Card: 10%** of account value  
**Twitter Creds: \$16, PayPal: Same as ATM**

# Blurred Boundaries between Work, Home Life Add Risk

**Do you use your personal device for work or work device for personal tasks like checking email?**



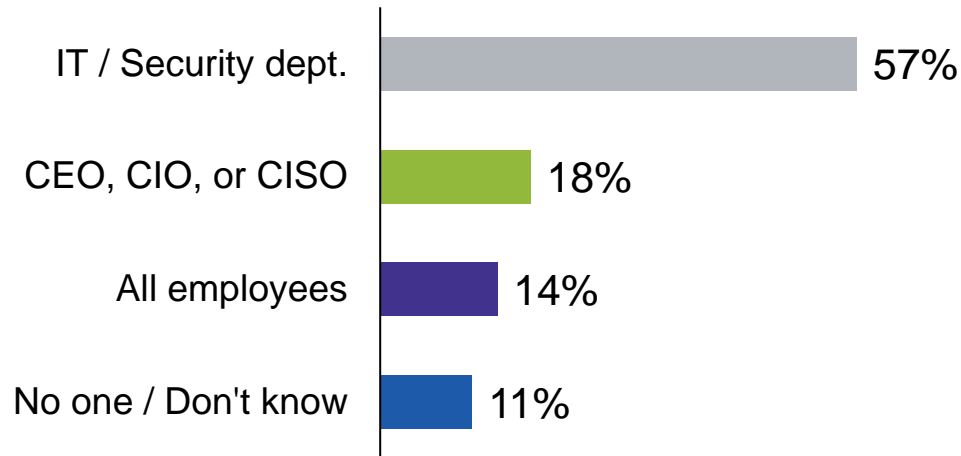
- Stress and mental health
- Distraction
- False sense of security
- Unsecured personal devices
- Doing personal tasks on work devices

*“People are taking increased physical safety measures in the pandemic, including mask wearing, more frequent hand-washing, etc. I think this heightened level of precaution and awareness could cause people to slightly overestimate their overall safety, including their safety regarding online threats.”*

– Prashanth Rajivan, Ph.D.

# “Not My Responsibility”

Who is responsible for cyber resilience in your company?

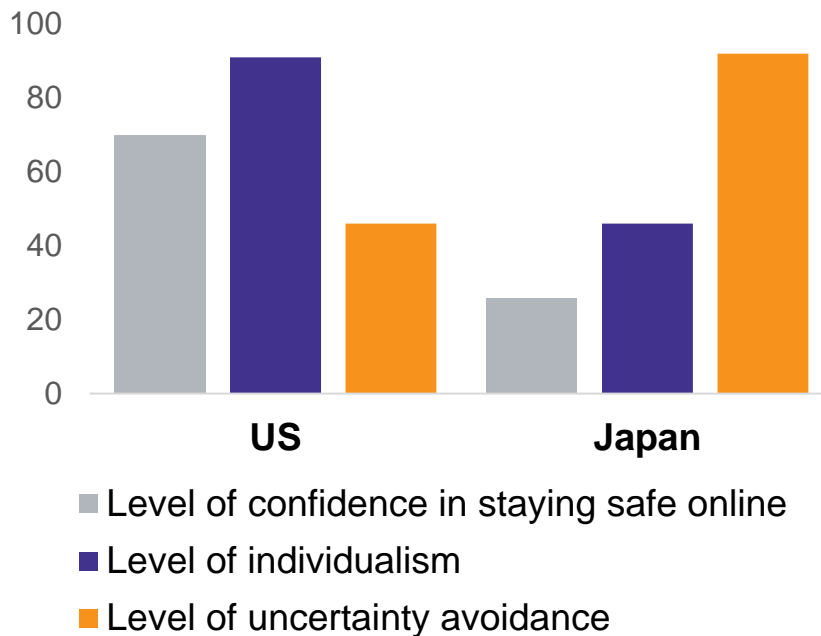
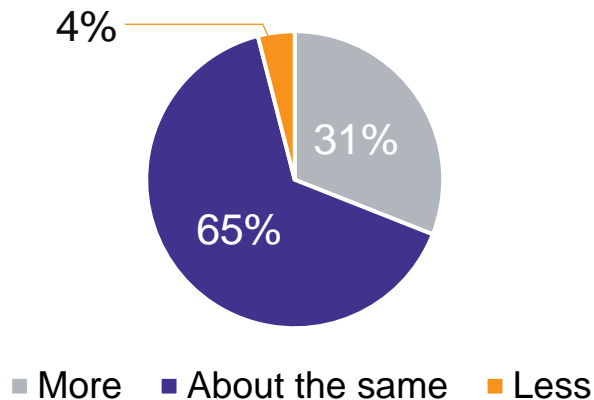


*“A company is vulnerable to attacks because each employee is vulnerable.”*

– Briana Butler, engineering services manager, Carbonite + Webroot, OpenText Companies

# Overconfidence

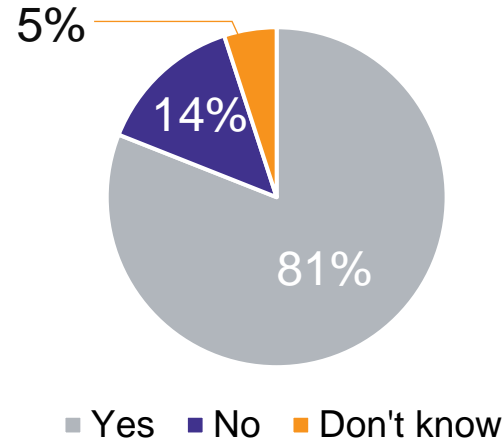
Given the increase in the amount of time you've spent working from home, do you feel more or less prepared to spot phishing email attempts?



# Ways to Identify High-Risk Users

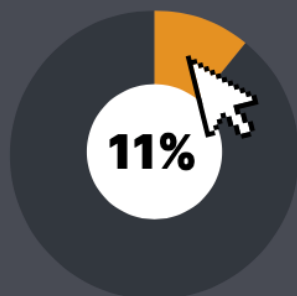
- Employee monitoring software
- Data loss prevention software
- See who interacts the most with the help desk
- Dark web breach reporting
- The tried-and-true method: phishing simulations

**When checking your email, do you take any steps to determine if an email message could be malicious?**



# Security Awareness Training Proves its Worth

The more phishing simulations you run, the more the click-through rates (%) improve.



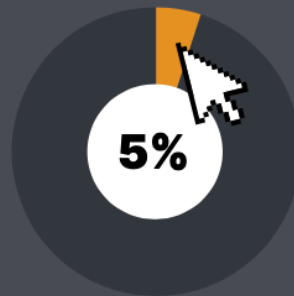
1 Phishing simulation



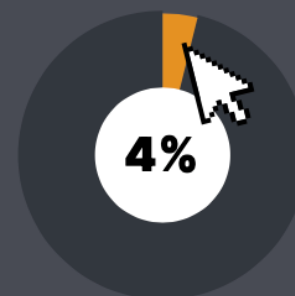
2-3 Phishing simulations



4-10 Phishing simulations



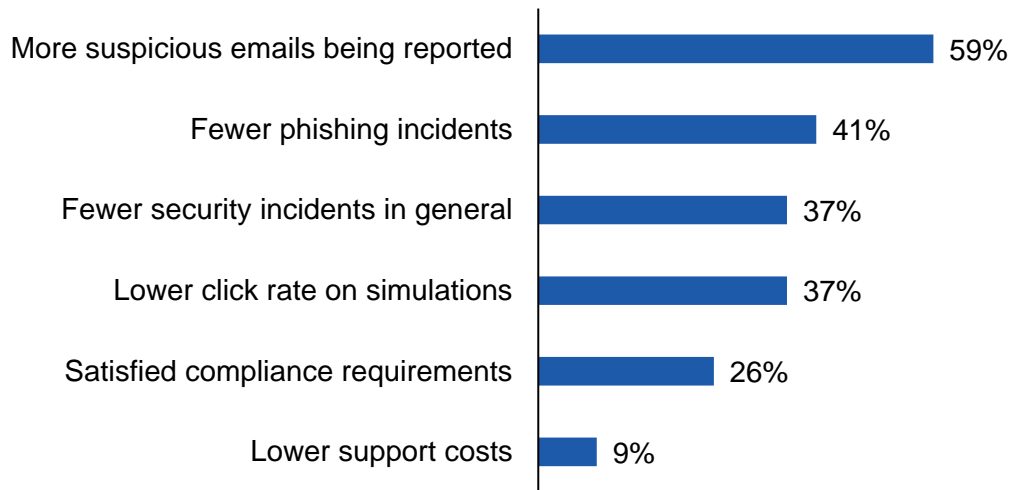
11-14 Phishing simulations



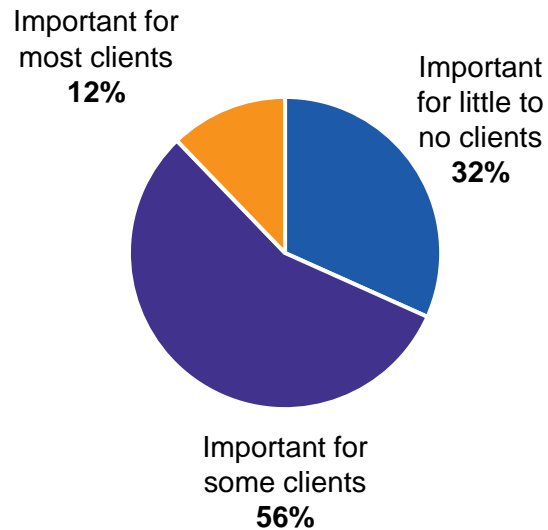
15-17 Phishing simulations

# Changing user behavior around email is the #1 benefit

Have you or your clients experienced any benefits from SAT?  
(Select all that apply)



How important are compliance requirements to justify SAT?

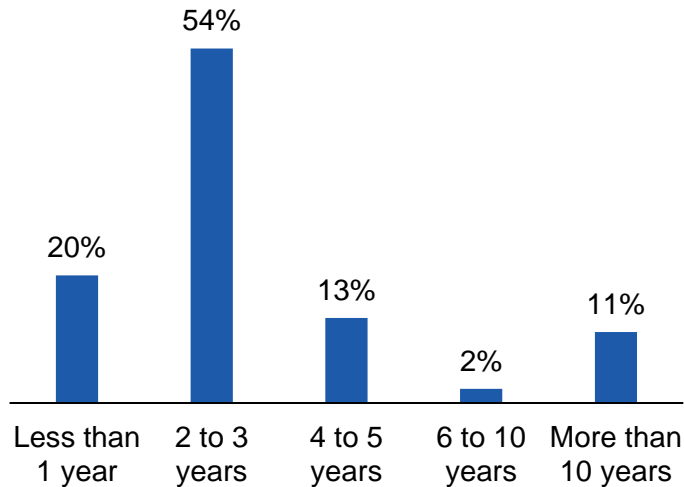


Base: 46 MSPs that provide Security Awareness Training | Source: November 2020 Webroot MSP SAT Survey

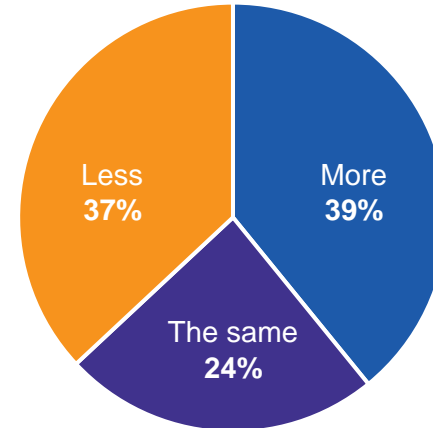


# Most have provided SAT for less than 3 years

## How Long Have You Been Providing SAT?



## Have You Delivered More (or Less) SAT in 2020?

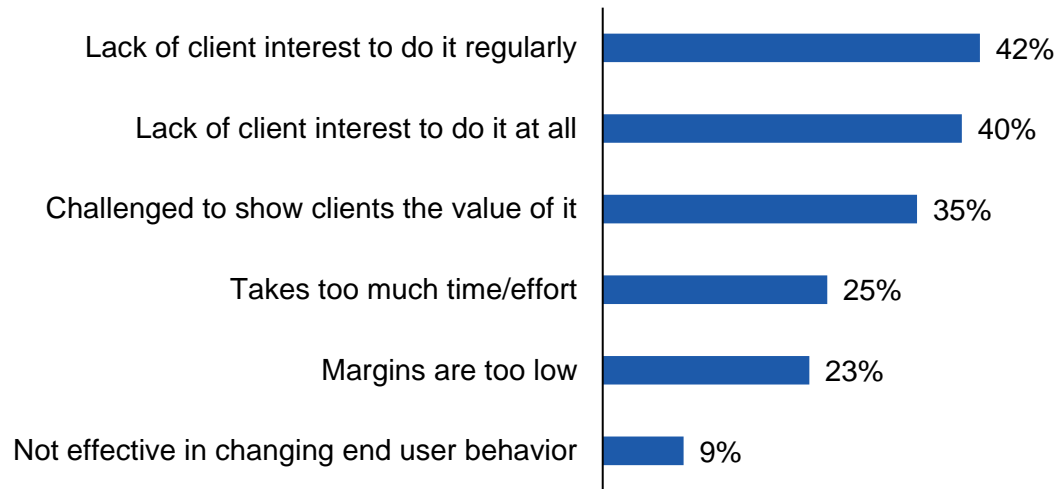


46% of respondents provide SAT to their clients

Base: 46 MSPs that provide Security Awareness Training | Source: November 2020 Webroot MSP SAT Survey

# Client interest remains the #1 barrier to adoption

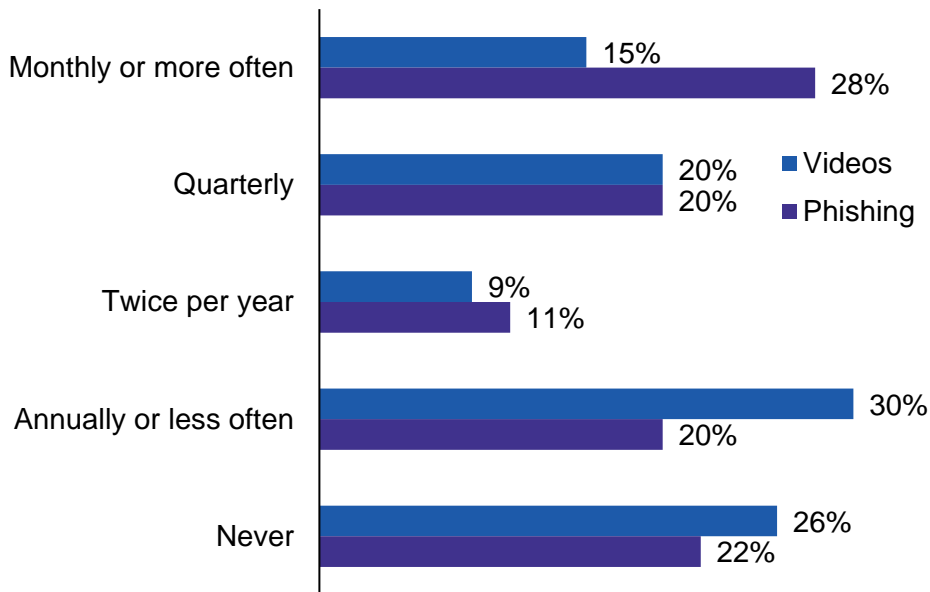
## Is anything preventing you from delivering more SAT? (Select all that apply)



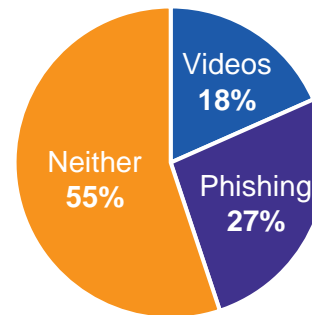
Base: 100 MSPs | Source: November 2020 Webroot MSP SAT Survey

# Simulated phishing gets more focus

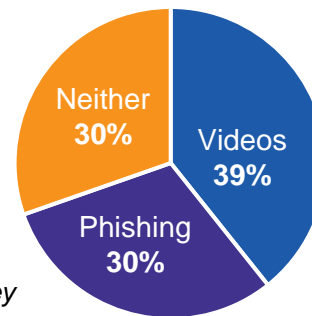
## How Often Do Clients Receive Training?



## Do You Target Specific Job Roles?

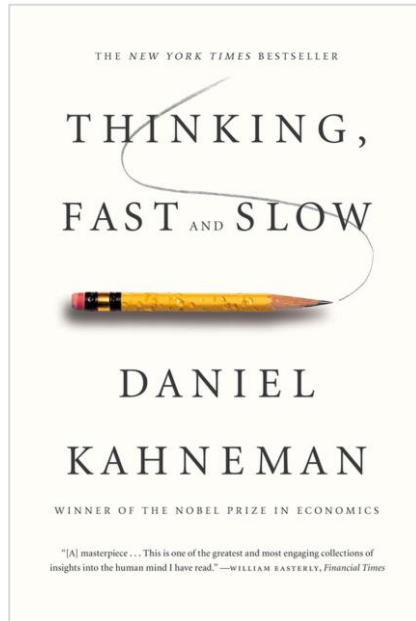


## Do You Target Simulated Phishing Victims?



Base: 46 MSPs that provide Security Awareness Training | Source: November 2020 Webroot MSP SAT Survey

# Encourage a More Reflective, Analytical Approach

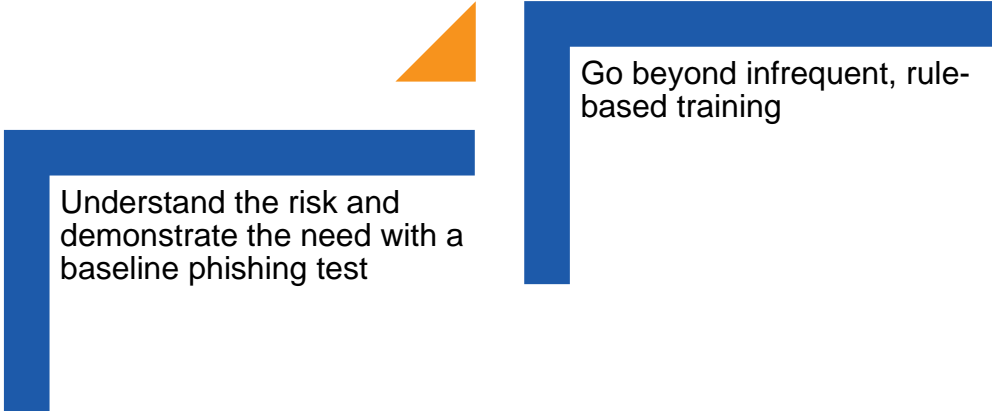


- Repetitive, rule-based training can be counter-productive
- Help employees develop a suspicious mindset
- Ongoing exercise and feedback is necessary to change behavior

*“Give a man a truth and he will think for a day. Teach a man to reason and he will think for a lifetime.”*

– Phil Plait

# Next Steps

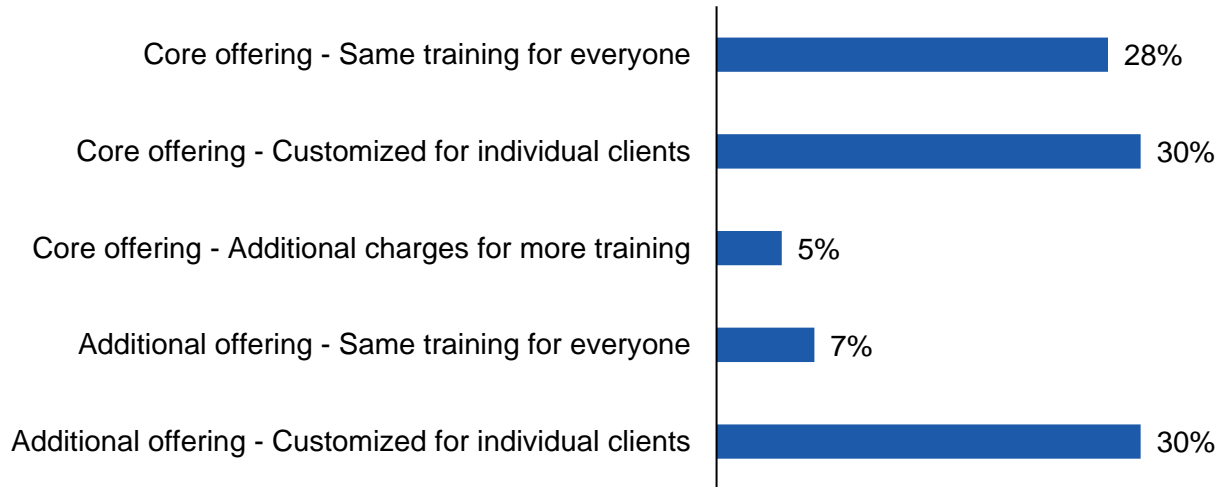


Understand the risk and demonstrate the need with a baseline phishing test

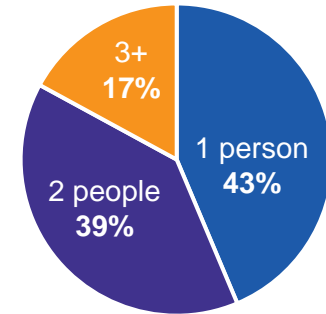
Go beyond infrequent, rule-based training

# Most include SAT in their core offering

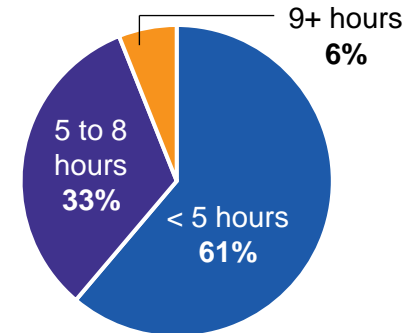
## How Do You Package SAT?



## Number of Staff Involved



## Monthly Hours Spent on SAT



Base: 46 MSPs that provide Security Awareness Training | Source: November 2020 Webroot MSP SAT Survey

**COVID CDC Spoof**

Sender Name: CDC INFO National Contact Center

Sender Address: CDC-info @ admin-alerts.com

Email Subject: CDC Health Alert: Updated Case List in Your City

Email Body:

Distributed via the CDC Health Alert Network  
 [[DATE]]  
 CDCHAN-00426

Dear [FIRSTNAME],

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at <https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html>

You are immediately advised to go through the cases above for safety hazard.

Sincerely,  
 CDC-INFO National Contact Center  
 National Center for Health Marketing  
 Division of eHealth Marketing  
 Centers for Disease Control and Prevention

Cancel Save as New Apply Edits

**COVID New Company Policy: Communicable Disease Management Policy**

Sender Name: Human Resources

Sender Address: CDC-info @ hr-internal.com

Email Subject: Communicable Disease Management Policy

Email Body:

All,

Due to the coronavirus outbreak, [[COMPANY NAME]] is actively taking safety precautions by insituting a [Communicable Disease Management Policy](#). This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy immediately.

If you have any questions or concerns regarding the policy, please contact [[COMPANY NAME]] Human Resources.

Regards,  
 Human Resources

Cancel Save as New Apply Edits

# Webroot® Security Awareness Training

One centralized solution for ongoing awareness training



## Phishing Simulator

- Test and **measure** user progress
- Identify high risk users
- 200+ up-to-date real-world phishing examples



## Training Courses

- Comprehensive library of security and compliance topics
- Award-winning training informed by threat intelligence and real-world events
- Monthly updates



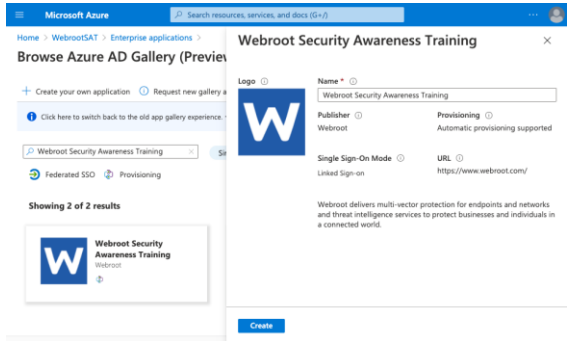
## Reporting/Compliance

- Integrated reporting center
- Dark Web Breach report for identifying high risk users
- Meets compliance **requirements** PCI, HIPAA, GDPR, CCPA

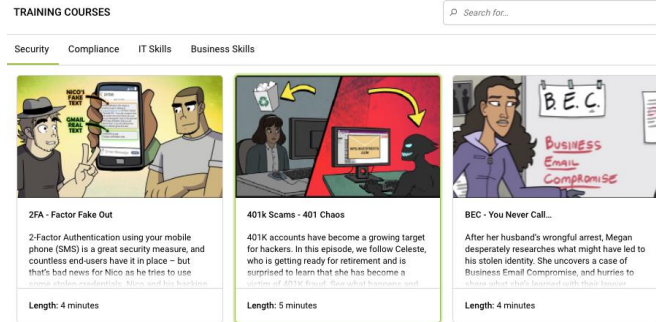


# Security Awareness Application (web-based)

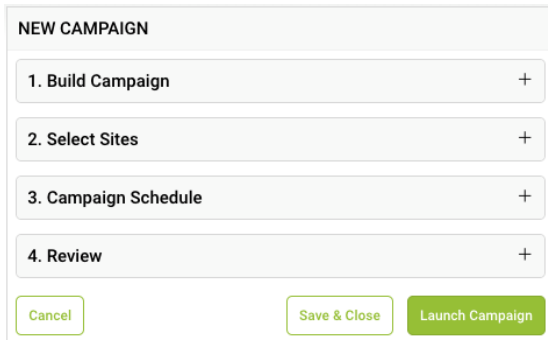
## Microsoft Azure AD integration for user import



## Content library to browse/discover available training

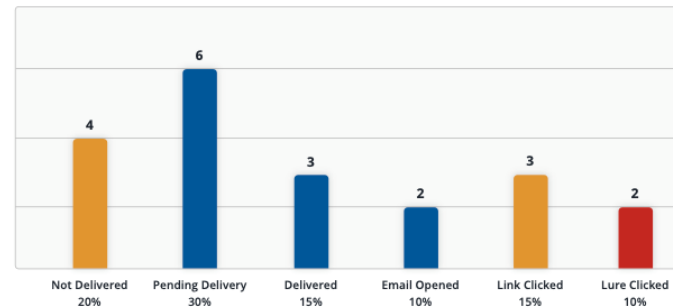


## Simple 4-step wizard to create a campaign



## See campaign results in reporting

Total Number of Users: 20



# Questions

If you take a 30-day free trial, we will send you a \$25 GrubHub gift card:

[bit.ly/TAGNov12WebinarTrials](https://bit.ly/TAGNov12WebinarTrials)



twitter.com/webroot



linkedin.com/company/webroot

PKarcher@OpenText.com