KnowBe4
Human error. Conquered.

Cyber Crime:
The Threat is Real!

State of North Carolina
Cyber Symposium - October 2021

Andrew Guay-ENT CSM & Kathleen Gardner-VP Customer Relations

DISCLAIMER: *This presentation contains simulated phishing attacks. The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes. The marks are property of their respective owners and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.*

Agenda

Intro to KnowBe4

Threat Intel

Cyberwarfare
NIST Recommendations

Engagement

Phishing Benchmarking 2021 Report
Assessments - Awareness & Culture
Value Adds & Resources

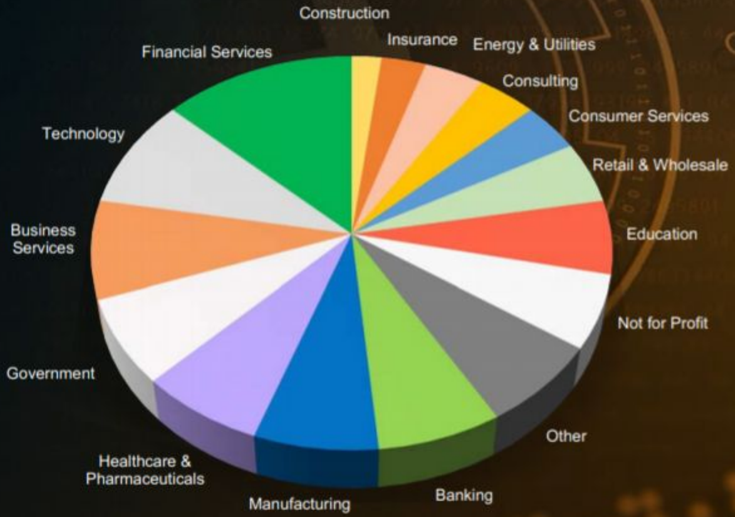
Demo Presentation

Building a Phishing/Training Campaign
Automation in the Platform - Ease of Use

KnowBe4
Human error. Conquered.

Over

40,000 Customers



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER WAVE LEADER 2020 Security Awareness And Training Solutions

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES Inc. 500

Gartner peerinsights company size—customers' choice 2021

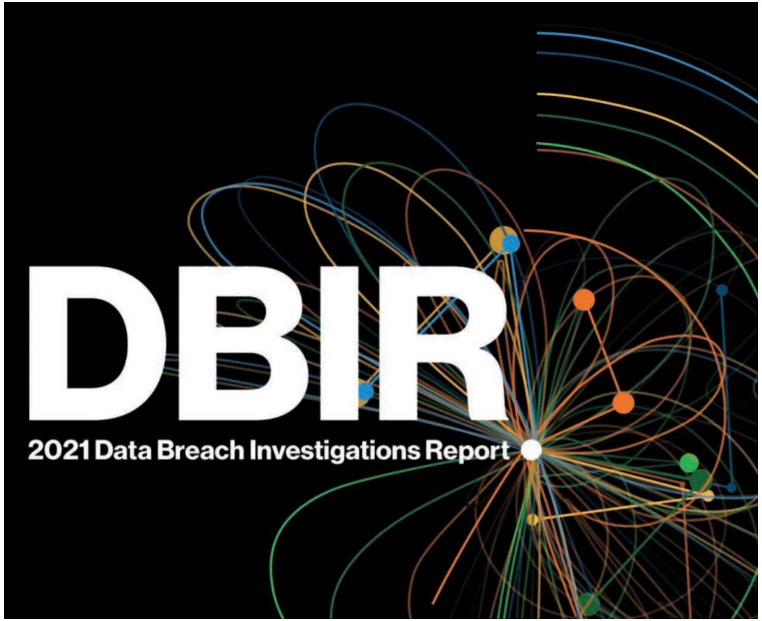
KnowBe4 Human error. Conquered.

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/0/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

National Cyber Security Centre
a part of GCHQ

CYBERSECURITY ADVISORY



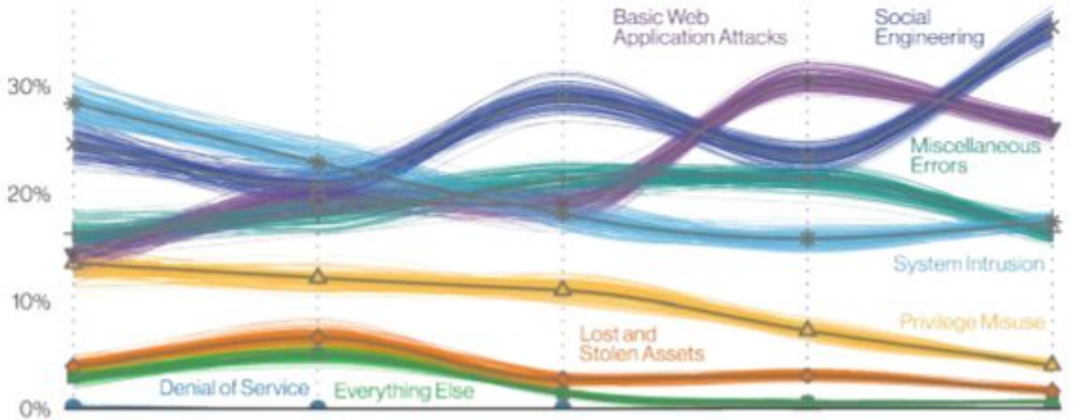
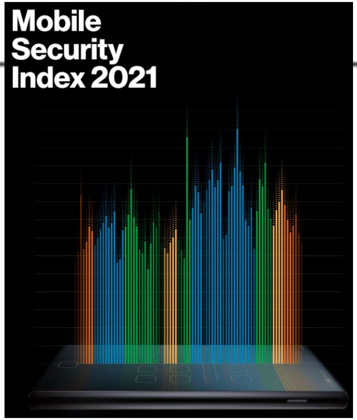


Figure 45. Patterns over time in breaches

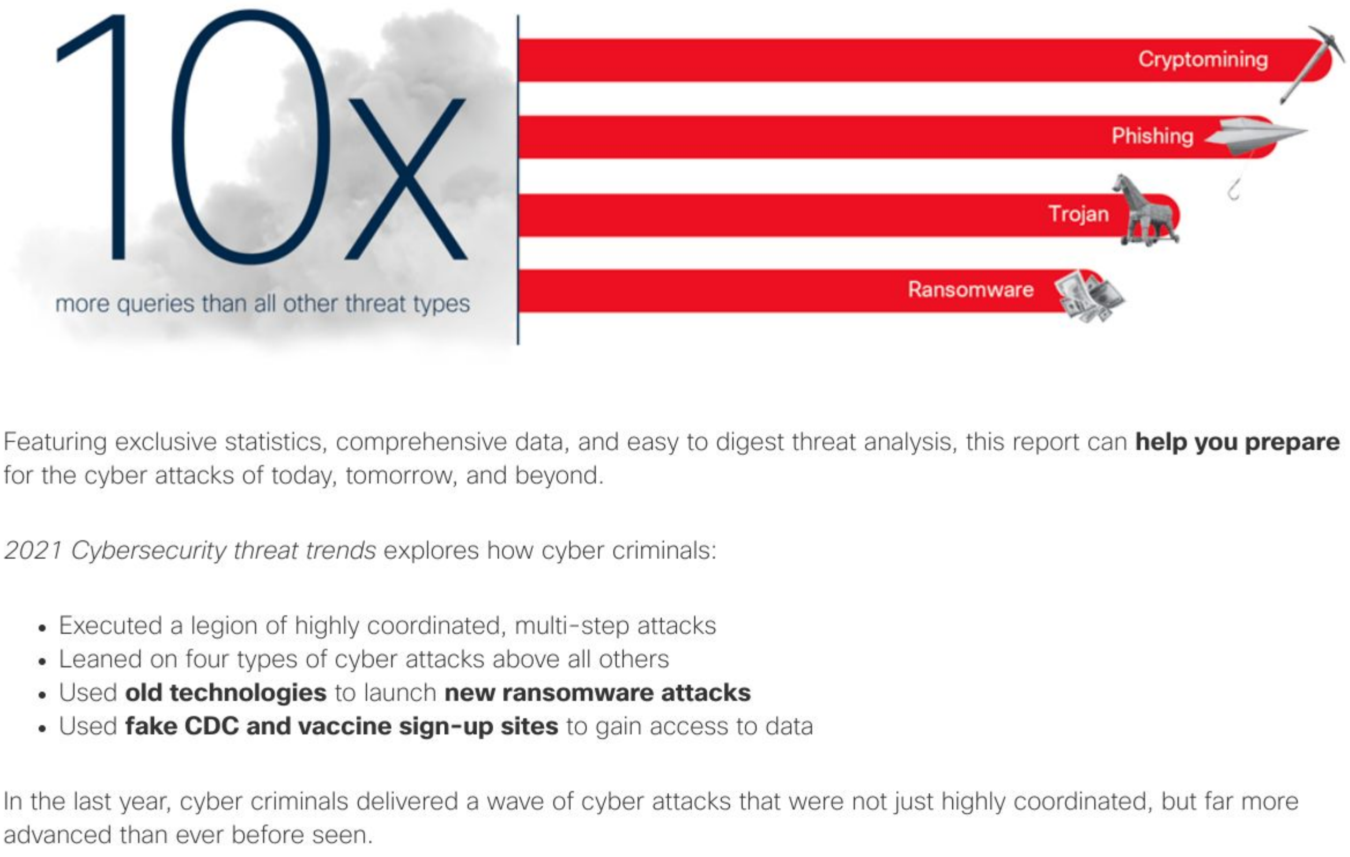


VERIZON'S 2021 DATA BREACH INVESTIGATION REPORT:

Verizon's latest report puts a spotlight on one of the largest and most unpredictable risk factors in your cybersecurity strategy - **your users…**

According to the Report: **PHISHING is #1 Threat Action (involved in 36% of breaches)**
85% of data breaches involved a human element! Approximately 1/3 of data breaches involve Social Engineering

Cisco’s Cybersecurity Threat Trends 2021 Report



Featuring exclusive statistics, comprehensive data, and easy to digest threat analysis, this report can **help you prepare** for the cyber attacks of today, tomorrow, and beyond.

2021 Cybersecurity threat trends explores how cyber criminals:

- Executed a legion of highly coordinated, multi-step attacks
- Leaned on four types of cyber attacks above all others
- Used **old technologies** to launch **new ransomware attacks**
- Used **fake CDC and vaccine sign-up sites** to gain access to data

In the last year, cyber criminals delivered a wave of cyber attacks that were not just highly coordinated, but far more advanced than ever before seen.

Cybersecurity threatscape

Q2 2021

ptsecurity.com

ptsecurity.com

Statistics

The # of attacks on governmental institutions (amongst all attacks on organizations) soared from 12% in Q12021 to 20% in Q22021

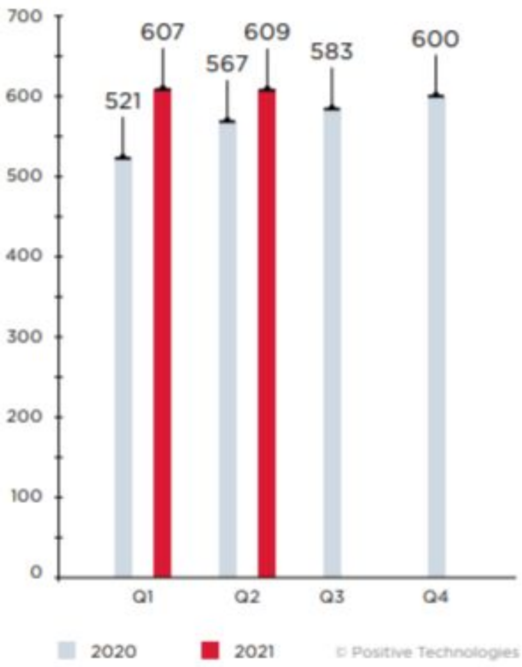


Figure 1. Number of attacks in 2020 and 2021 (per quarter)

77% of attacks were targeted

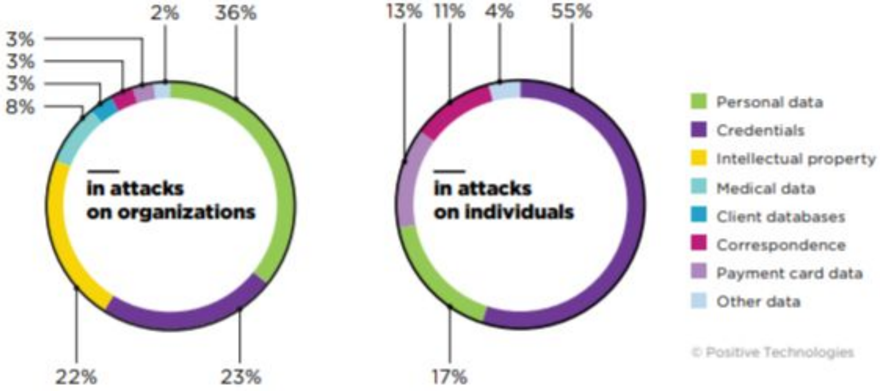


Figure 3. Types of data stolen

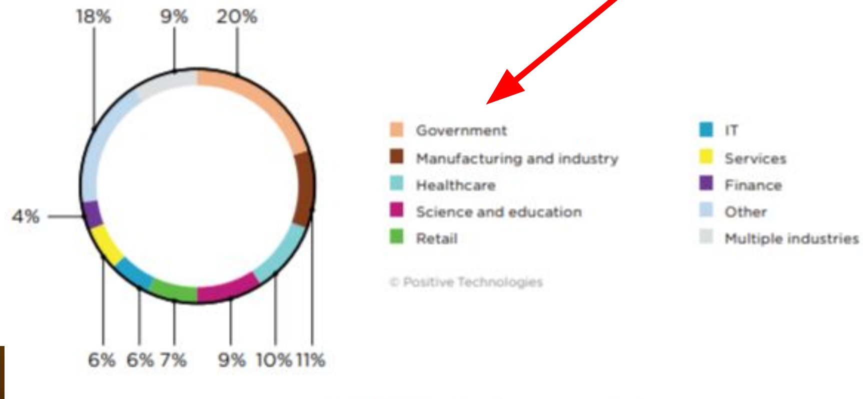


Figure 4. Victim categories among organizations

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SP 800-53 Rev. 5 Security & Privacy Controls for Information Systems & Organizations:
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Critical New Language to Sections Covering Security Awareness

- Provide Frequent Simulated Social Engineering Testing to include “providing practical exercises no-notice attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious em attachments or invoking, via spear phishing attacks, malicious web links”
- NIST Recommendation - NO NOTICE
- NIST Recommendation - NOT ONE-DIMENSIONAL
- NIST Recommendation - INC HIGHLY CRAFTED SPEAR PHISHING ATTACKS

In essence, NIST is saying your simulated social engineering testing needs to reflect real world threats so that you have a true understanding of your susceptibility to such threats!

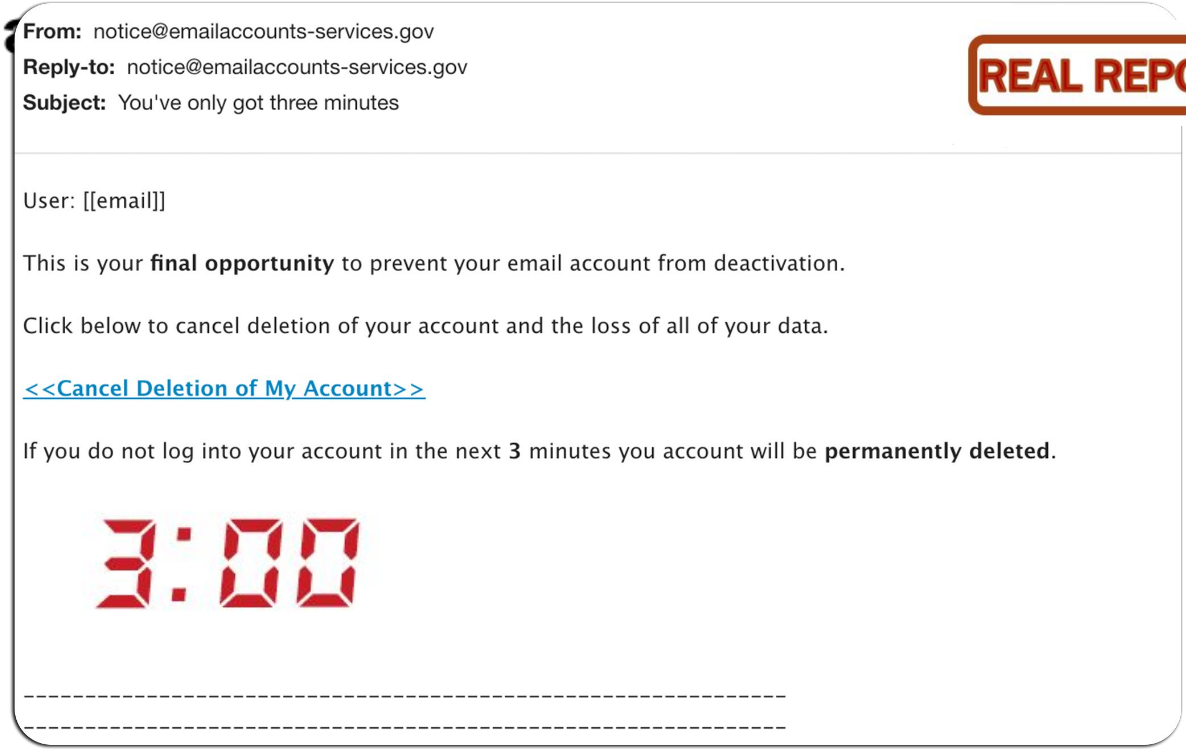
What techniques do hackers use most of the time?

According to our research, the majority of the emails that are reported to us use social engineering schemes that have been around for many years.

- **Fake invoices, POs, and RFQs**
  - “Your invoice is past due. Click here to pay it now.”
- **Fake package/parcel delivery notifications**
- **Fake file delivery/sharing/signing notifications**
- **Bogus online account verifications/updates**
- **Email upgrade/update notifications**
  - “Your email is due for upgrade. Upgrade your email or ALL emails will be deleted. UPGRADE NOW.”
- **Email password expiration notifications**
  - “Your password is expired. Enter your account portal now to create your new password so you can log in.”
- **Email deactivation warnings**
  - “Your email will be deactivated if you don’t click here to cancel deactivation.”

Most Interesting Phishing Techniques: Timer

example of actual phishing email received @ KnowBe4



From: notice@emailaccounts-services.gov

Reply-to: notice@emailaccounts-services.gov

Subject: You've only got three minutes

User: [[email]]

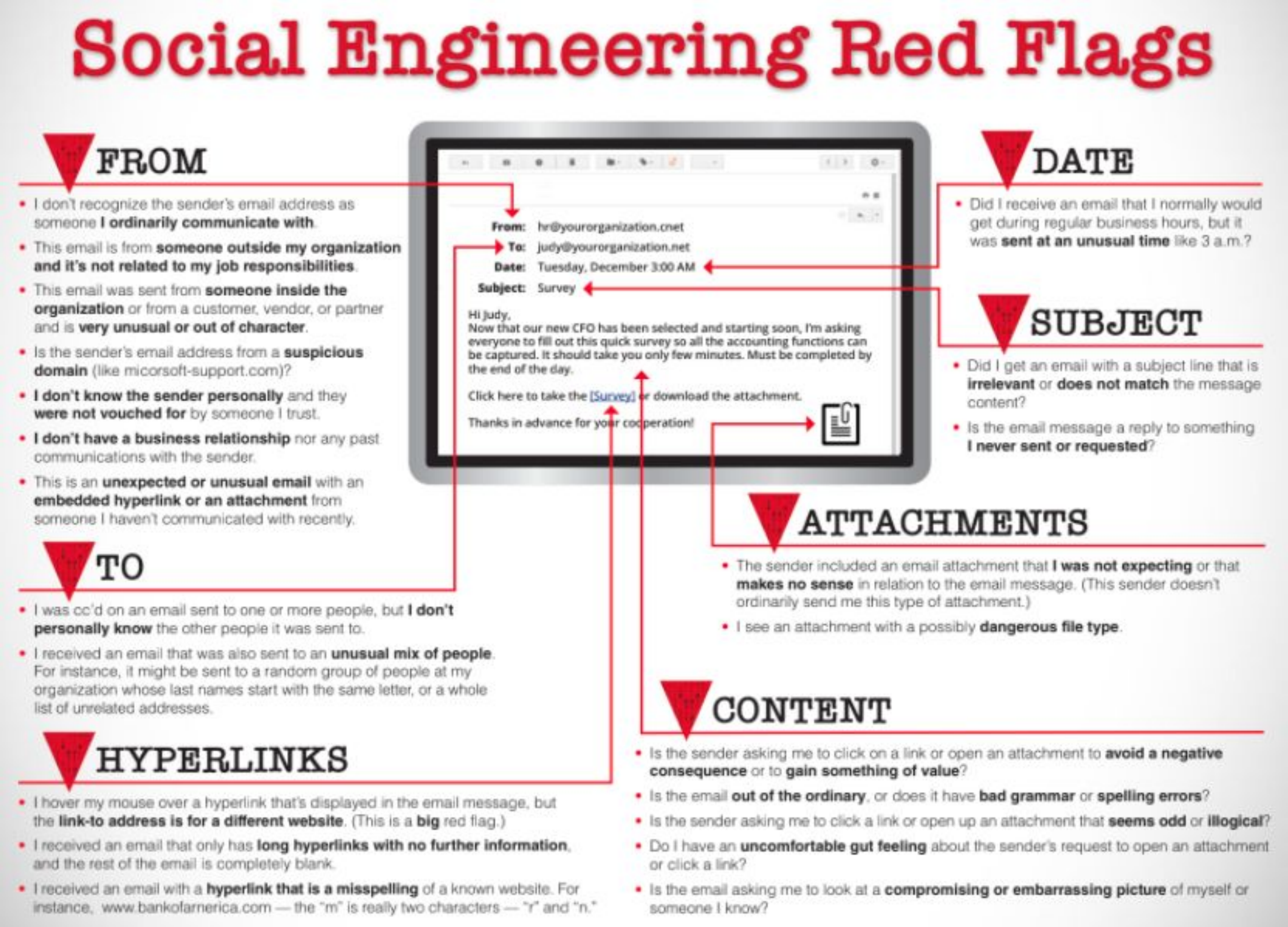
This is your **final opportunity** to prevent your email account from deactivation.

Click below to cancel deletion of your account and the loss of all of your data.

<<Cancel Deletion of My Account>>

If you do not log into your account in the next **3** minutes you account will be **permanently deleted**.

REAL REPORTED PHISH



Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Survey

Hi Judy,
Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

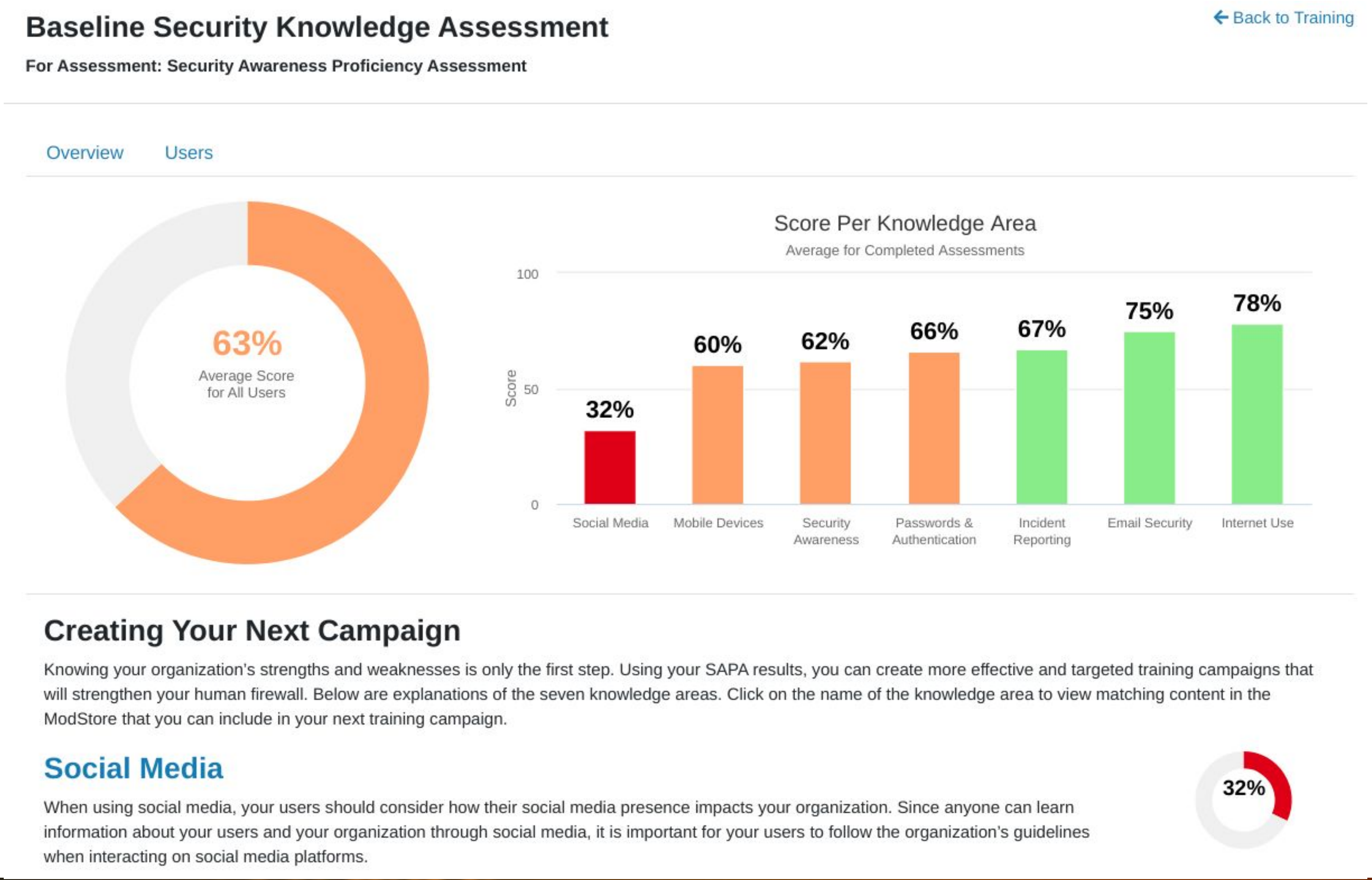
CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Security Awareness Proficiency Assessment

Available in the Modstore!

Know where to tailor your training campaigns!



← Back to Training

Baseline Security Knowledge Assessment

For Assessment: Security Awareness Proficiency Assessment

Overview Users

Creating Your Next Campaign

Knowing your organization's strengths and weaknesses is only the first step. Using your SAPA results, you can create more effective and targeted training campaigns that will strengthen your human firewall. Below are explanations of the seven knowledge areas. Click on the name of the knowledge area to view matching content in the ModStore that you can include in your next training campaign.

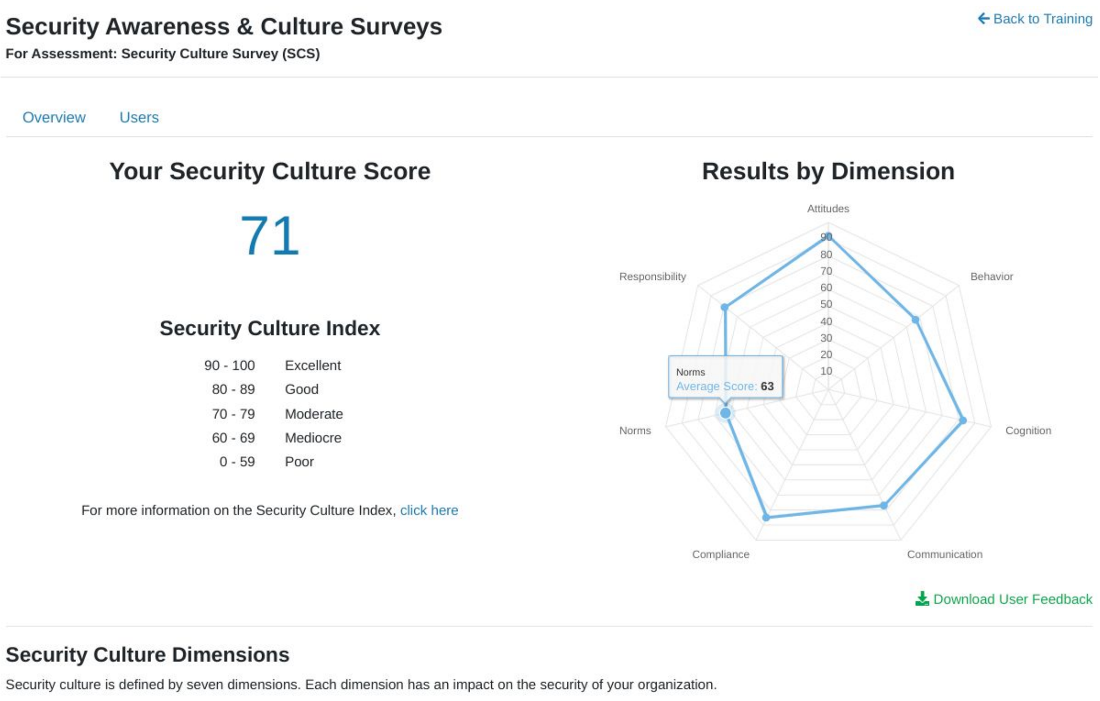
Social Media

When using social media, your users should consider how their social media presence impacts your organization. Since anyone can learn information about your users and your organization through social media, it is important for your users to follow the organization's guidelines when interacting on social media platforms.

Security Culture Survey

KnowBe4 Research
CLTRe
The Security Culture Report 2021
A Global Security Culture Perspective During a Pandemic

KnowBe4 Research



Security Awareness & Culture Surveys

For Assessment: Security Culture Survey (SCS)

← Back to Training

Overview   Users

Your Security Culture Score

71

Security Culture Index

90 - 100	Excellent
80 - 89	Good
70 - 79	Moderate
60 - 69	Mediocre
0 - 59	Poor

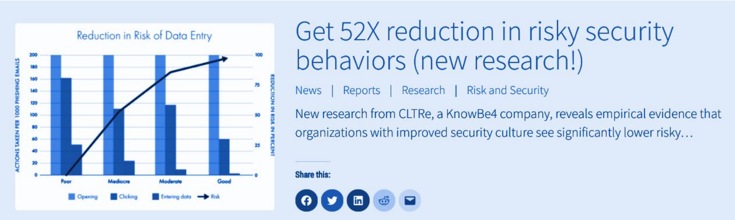
For more information on the Security Culture Index, click here

Results by Dimension

Download User Feedback

Security Culture Dimensions

Security culture is defined by seven dimensions. Each dimension has an impact on the security of your organization.


Reduction in Risk of Data Entry
ACTIONS TAKEN PER 1000 PHISHING EMAILS
200
180
160
140
120
100
80
60
40
20
0
REDUCTION IN RISK IN PERCENT
100
75
50
25
0
Poor
Mediocre
Moderate
Good
Opening
Clicking
Entering data
Risk

Get 52X reduction in risky security behaviors (new research!)

News | Reports | Research | Risk and Security

New research from CLTRe, a KnowBe4 company, reveals empirical evidence that organizations with improved security culture see significantly lower risky…

Share this:

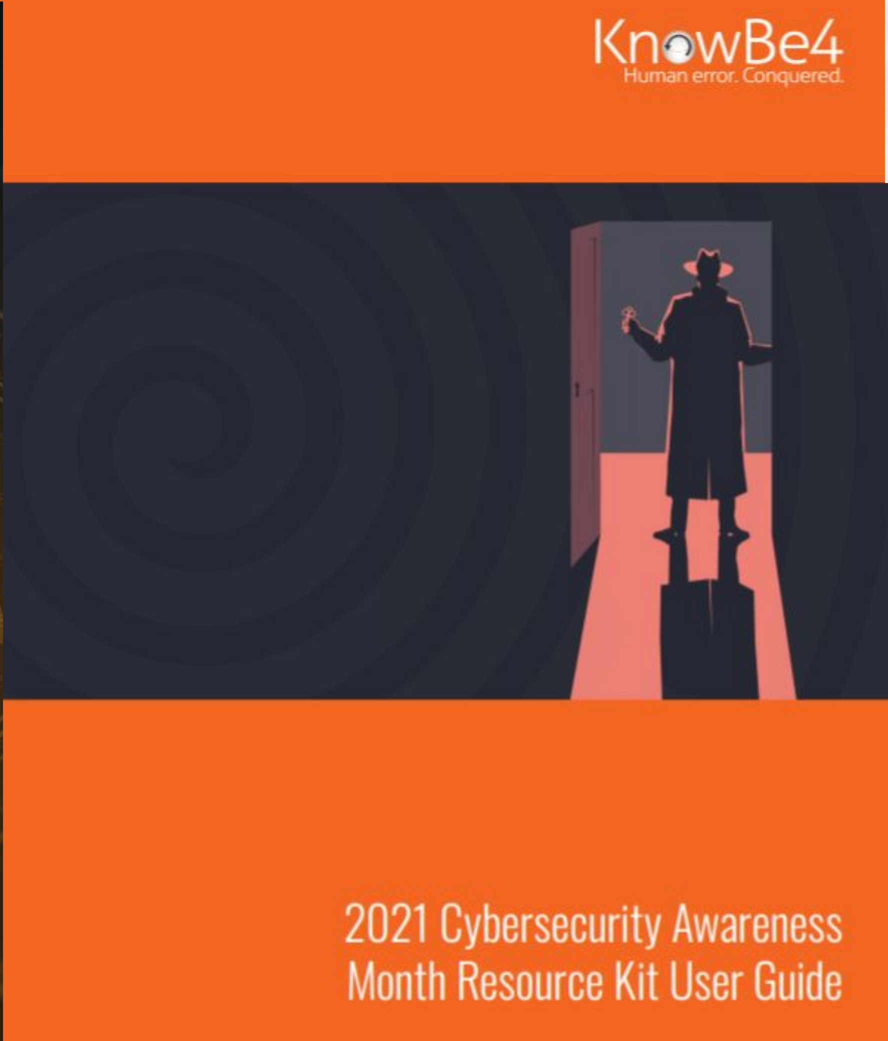
RESOURCES...

Cybersecurity Awareness Kit is out for October!

Developing a Successful SA Program - 5 Part Series:

https://support.knowbe4.com/hc/en-us/articles/4406863822483#h_01FFGCHGPA58A26AM2J0DMDE2X

KnowBe4
Human error. Conquered.

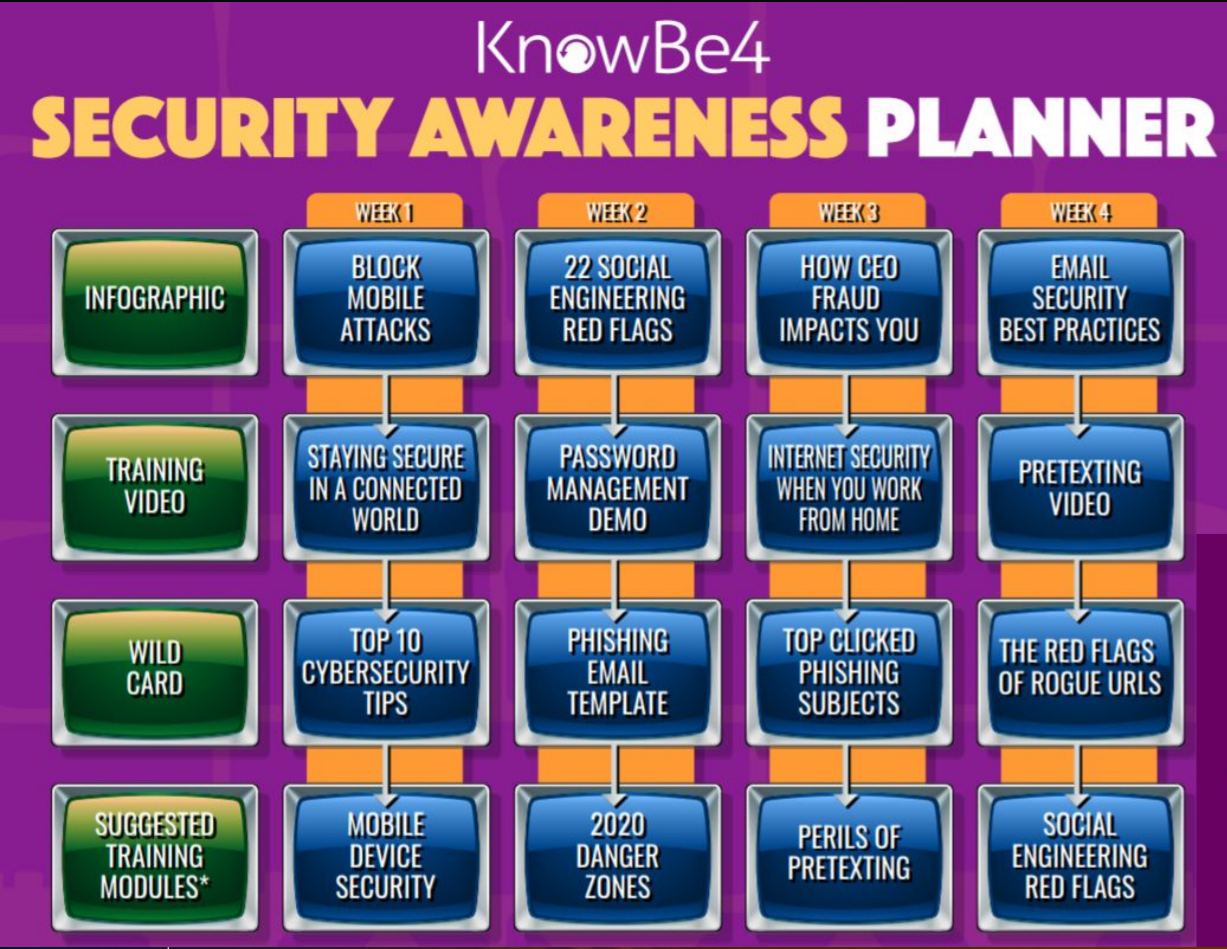


KnowBe4
Human error. Conquered.

2021 Cybersecurity Awareness Month Resource Kit User Guide

KnowBe4
Cybersecurity Awareness Weekly Training Planner

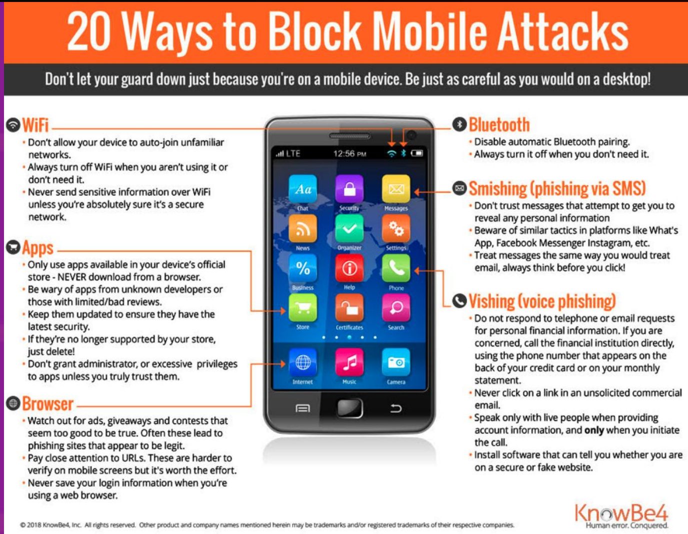
- On-Demand Webinar
- E-Book
- Interactive Weekly Planner
- Interactive Courses
- Videos
- 4 Infographics
- 4 Tip Sheets
- 4 Posters/Digital Signage



KnowBe4

SECURITY AWARENESS PLANNER

	WEEK 1	WEEK 2	WEEK 3	WEEK 4
INFOGRAPHIC	BLOCK MOBILE ATTACKS	22 SOCIAL ENGINEERING RED FLAGS	HOW CEO FRAUD IMPACTS YOU	EMAIL SECURITY BEST PRACTICES
TRAINING VIDEO	STAYING SECURE IN A CONNECTED WORLD	PASSWORD MANAGEMENT DEMO	INTERNET SECURITY WHEN YOU WORK FROM HOME	PRETEXTING VIDEO
WILD CARD	TOP 10 CYBERSECURITY TIPS	PHISHING EMAIL TEMPLATE	TOP CLICKED PHISHING SUBJECTS	THE RED FLAGS OF ROGUE URLS
SUGGESTED TRAINING MODULES*	MOBILE DEVICE SECURITY	2020 DANGER ZONES	PERILS OF PRETEXTING	SOCIAL ENGINEERING RED FLAGS



20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

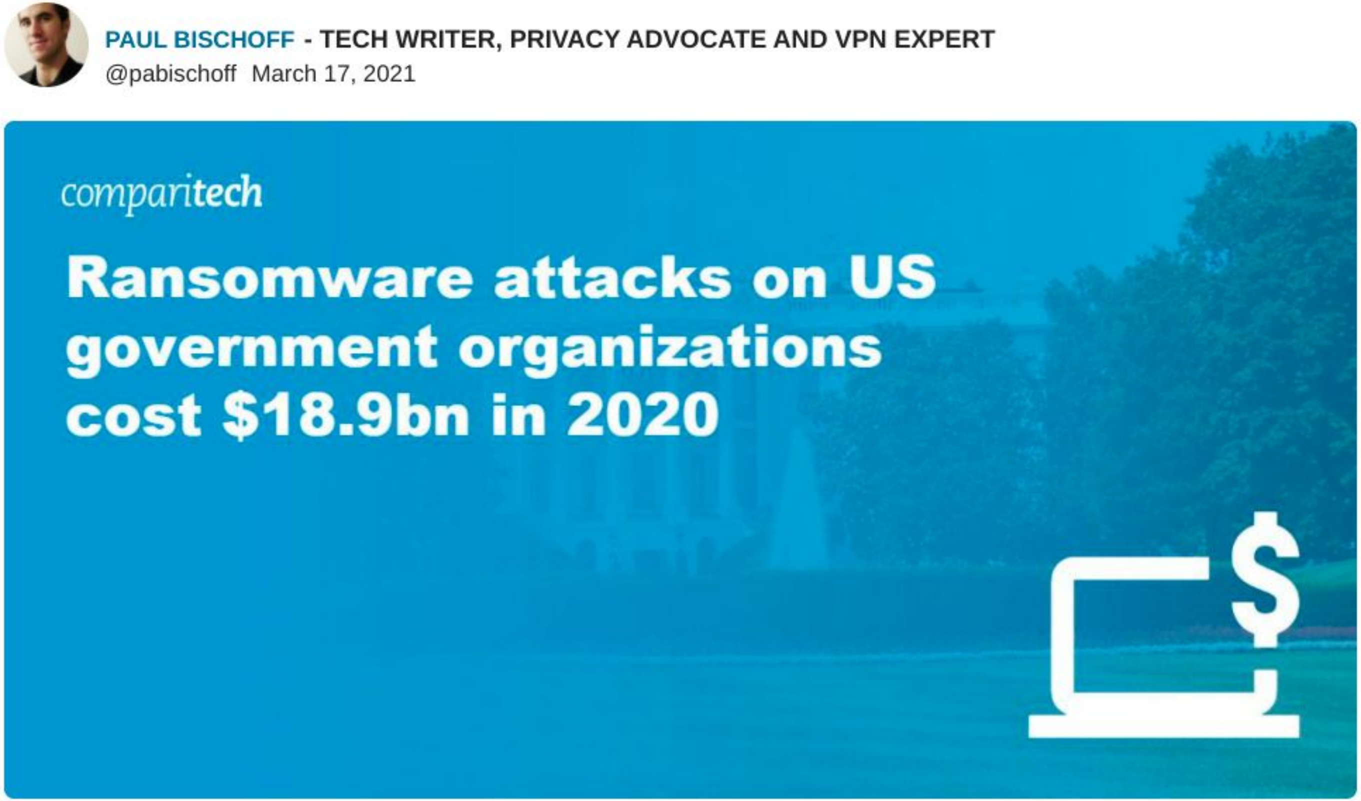
- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

KnowBe4
Human error. Conquered.

CEO FRAUD

WHO IS THAT EMAIL REALLY FROM?

KnowBe4
Human error. Conquered.



PAUL BISCHOFF - TECH WRITER, PRIVACY ADVOCATE AND VPN EXPERT
@pabischoff March 17, 2021

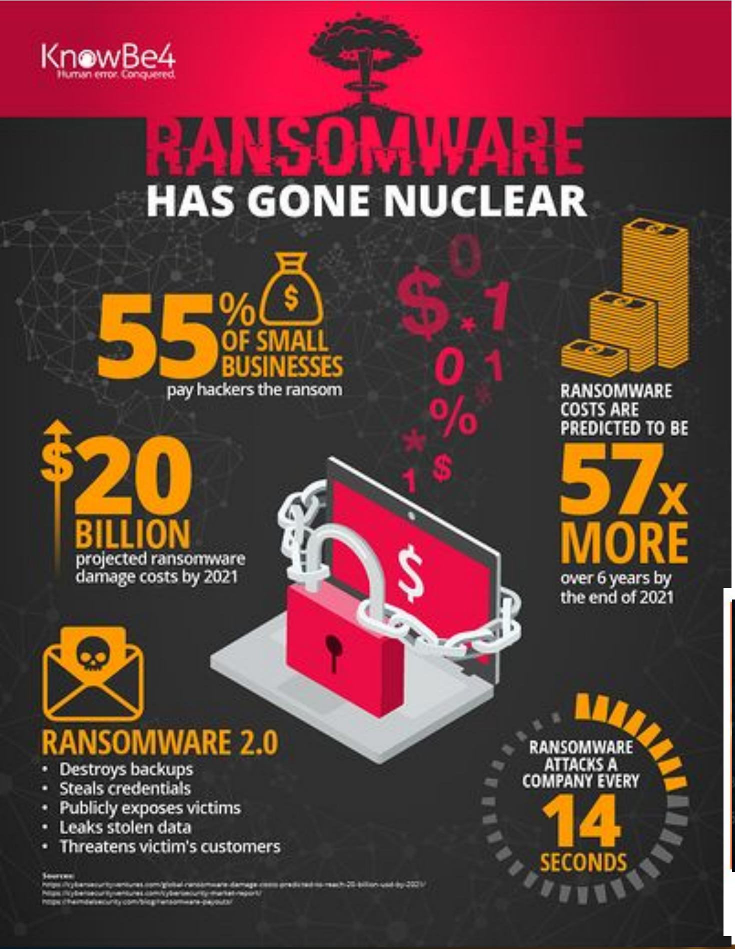
comparitech

Ransomware attacks on US government organizations cost $18.9bn in 2020

In 2020, 79 individual ransomware attacks were carried out against US government organizations, potentially impacting 71m people & costing an est'd $18.88 billion in downtime and recovery costs.

Over the last few years, ransomware has become a huge cause for concern. For gov entities, it can mean extended downtime, lost files, and the inability to access key infrastructure and services, including 911 and utilities.

https://www.comparitech.com/blog/information-security/government-ransomware-attacks/



RANSOMWARE HAS GONE NUCLEAR

55% OF SMALL BUSINESSES pay hackers the ransom

RANSOMWARE COSTS ARE PREDICTED TO BE 57x MORE over 6 years by the end of 2021

$20 BILLION projected ransomware damage costs by 2021

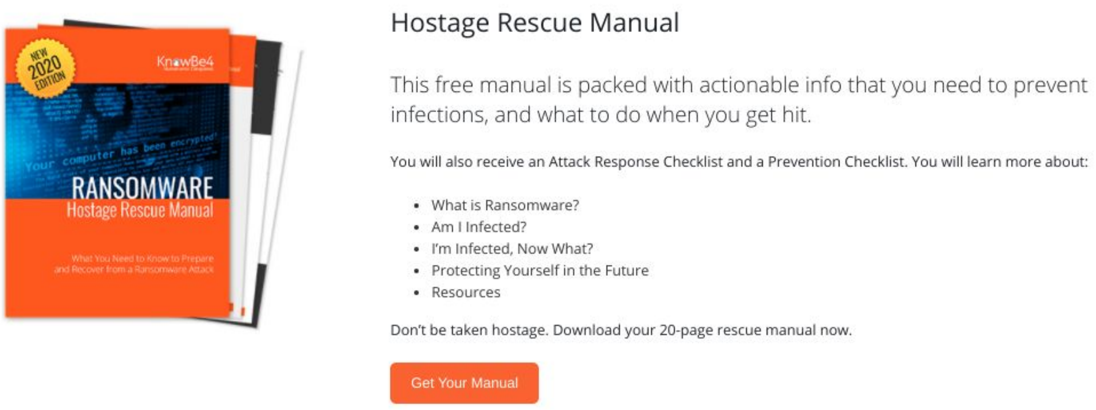
RANSOMWARE 2.0

- Destroys backups
- Steals credentials
- Publicly exposes victims
- Leaks stolen data
- Threatens victim's customers

RANSOMWARE ATTACKS A COMPANY EVERY 14 SECONDS

Sources:
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://cybersecurityventures.com/cybersecurity-market-report/
https://themidsecurity.com/blog/ransomware-payouts/

https://www.knowbe4.com/ransomware



NEW 2020 EDITION
KnowBe4
Your computer has been encrypted
RANSOMWARE
Hostage Rescue Manual
What You Need to Know to Prepare and Recover from a Ransomware Attack

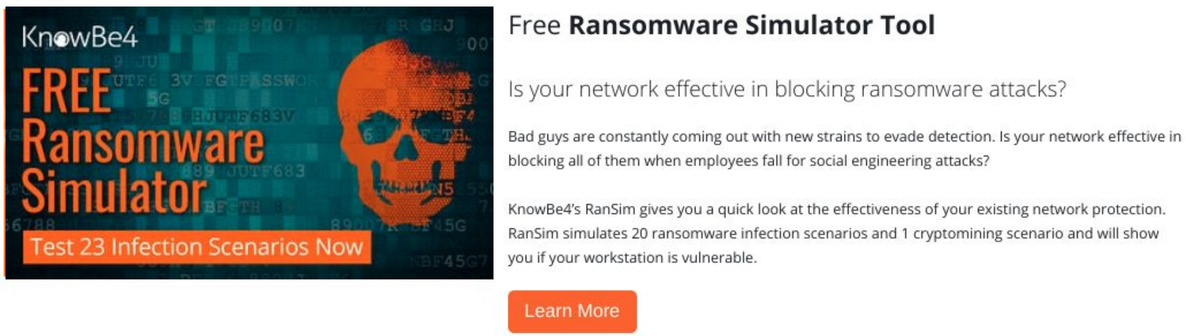
Hostage Rescue Manual

This free manual is packed with actionable info that you need to prevent infections, and what to do when you get hit.

You will also receive an Attack Response Checklist and a Prevention Checklist. You will learn more about:

- What is Ransomware?
- Am I Infected?
- I'm Infected, Now What?
- Protecting Yourself in the Future
- Resources

Don't be taken hostage. Download your 20-page rescue manual now.



Free **Ransomware Simulator Tool**

Is your network effective in blocking ransomware attacks?

Bad guys are constantly coming out with new strains to evade detection. Is your network effective in blocking all of them when employees fall for social engineering attacks?

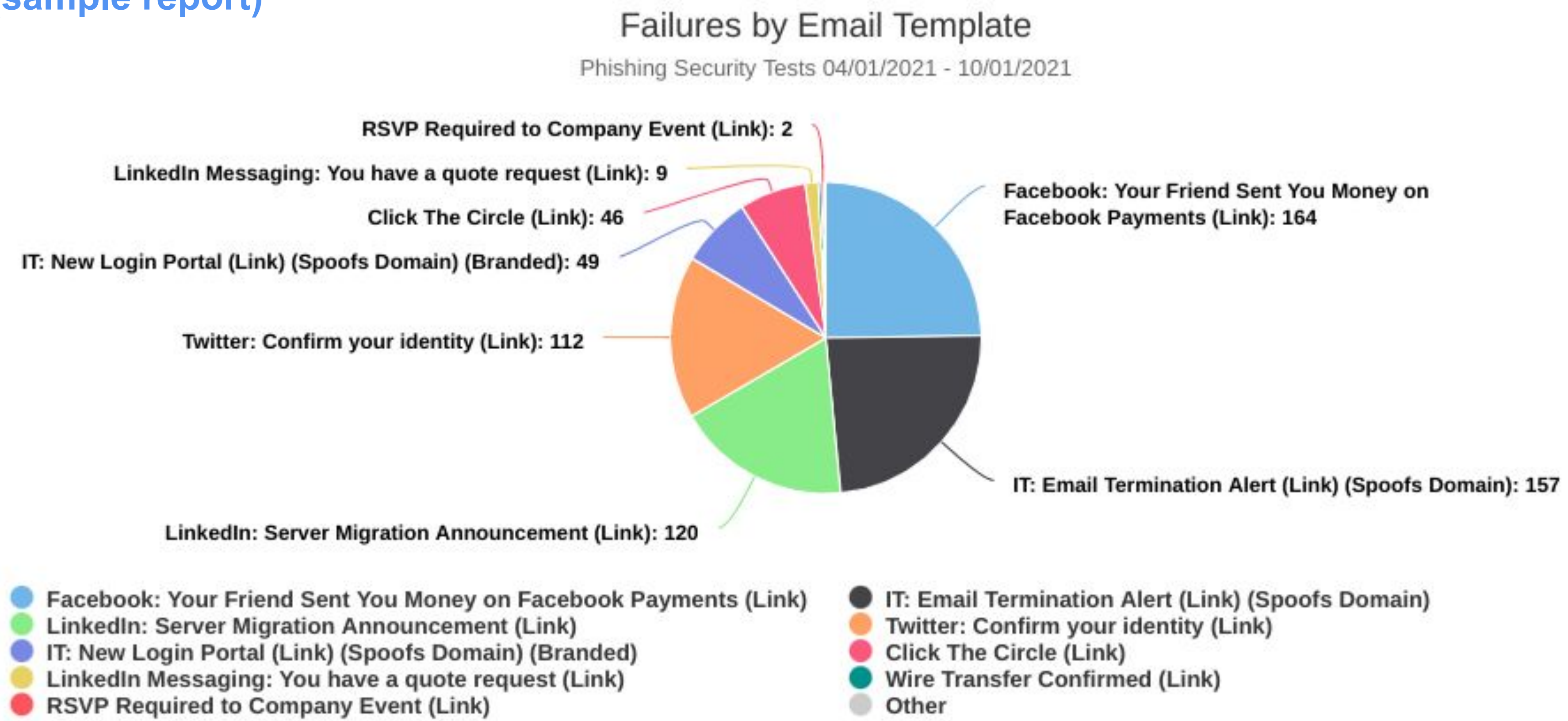
KnowBe4's RanSim gives you a quick look at the effectiveness of your existing network protection. RanSim simulates 20 ransomware infection scenarios and 1 cryptomining scenario and will show you if your workstation is vulnerable.

KnowBe4
Human error. Conquered.

Live Demo

KnowBe4 Console

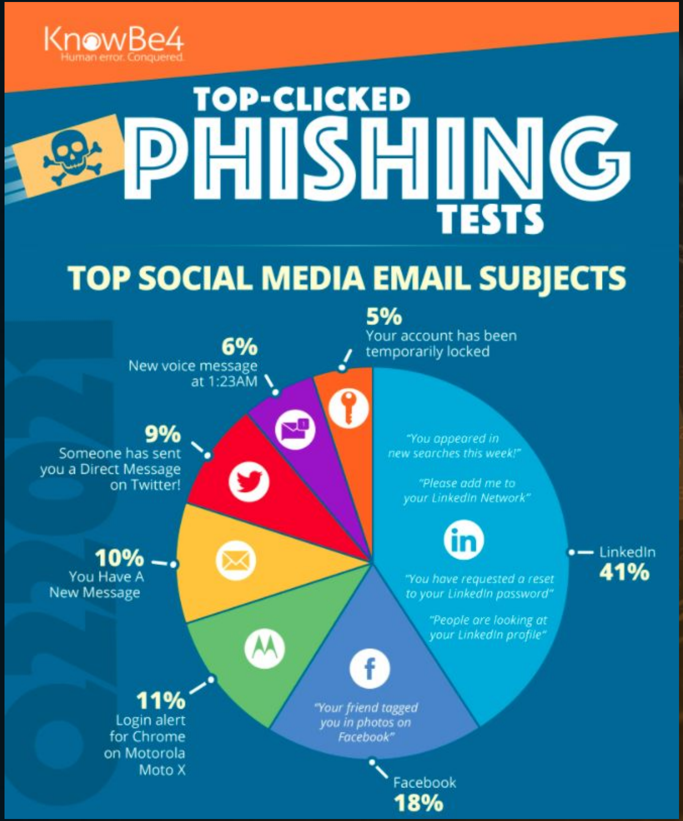
ADVANCED REPORTING...what type of phishing emails are your users clicking on? (sample report)



KnowBe4 RESOURCES...

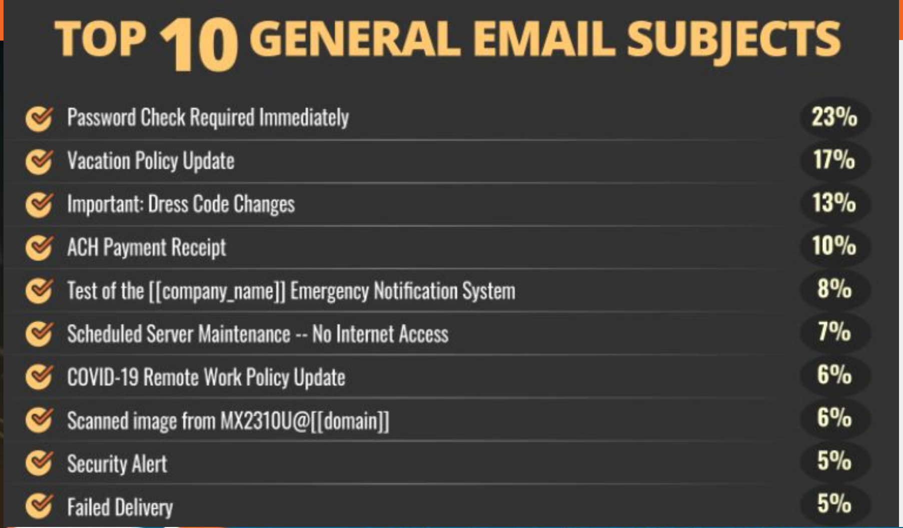
Q2 2021

Top 10 Reported Suspicious Emails



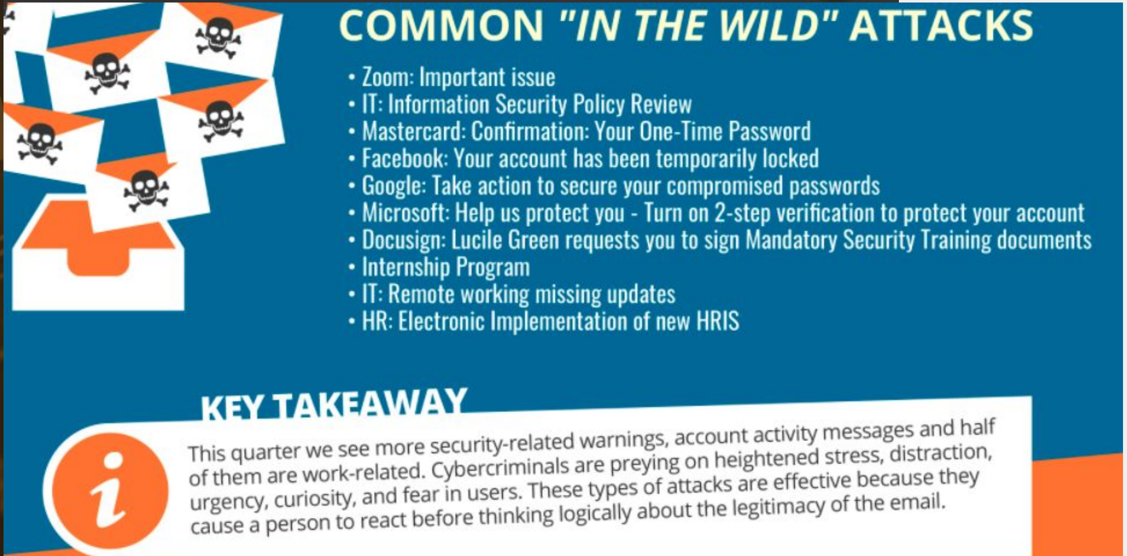
TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

✓ Password Check Required Immediately	23%
✓ Vacation Policy Update	17%
✓ Important: Dress Code Changes	13%
✓ ACH Payment Receipt	10%
✓ Test of the [[company_name]] Emergency Notification System	8%
✓ Scheduled Server Maintenance -- No Internet Access	7%
✓ COVID-19 Remote Work Policy Update	6%
✓ Scanned image from MX2310U@[[domain]]	6%
✓ Security Alert	5%
✓ Failed Delivery	5%



COMMON "IN THE WILD" ATTACKS

- Zoom: Important issue
- IT: Information Security Policy Review
- Mastercard: Confirmation: Your One-Time Password
- Facebook: Your account has been temporarily locked
- Google: Take action to secure your compromised passwords
- Microsoft: Help us protect you - Turn on 2-step verification to protect your account
- Docusign: Lucile Green requests you to sign Mandatory Security Training documents
- Internship Program
- IT: Remote working missing updates
- HR: Electronic Implementation of new HRIS

KEY TAKEAWAY

This quarter we see more security-related warnings, account activity messages and half of them are work-related. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

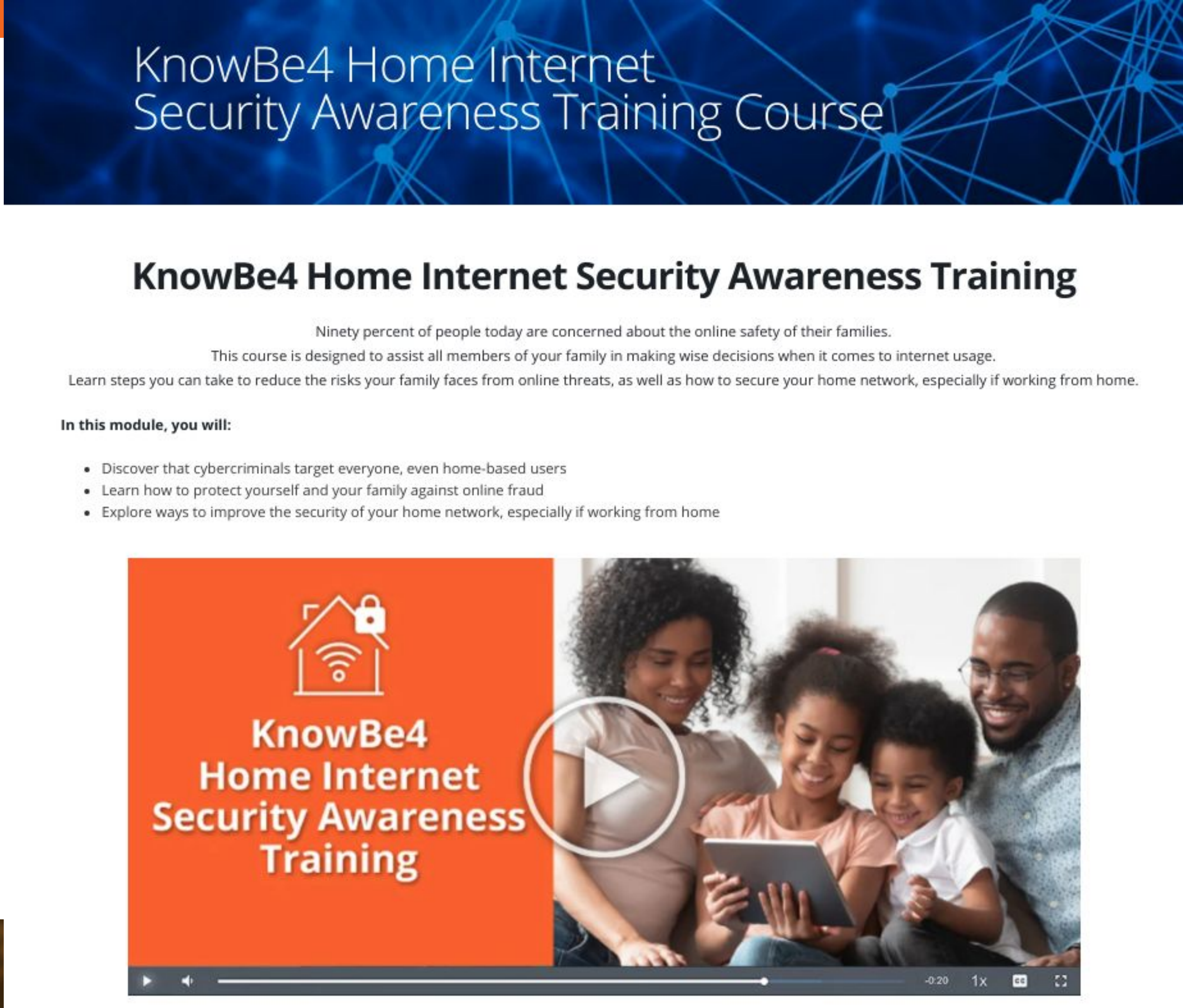
NEW Homecourse

knowbe4.com/homecourse

Password: homecourse

Share this free resource with your friends & families...Security Awareness starts in the home!

Reduce risks your family faces.



KnowBe4 Home Internet Security Awareness Training Course

KnowBe4 Home Internet Security Awareness Training

Ninety percent of people today are concerned about the online safety of their families.
This course is designed to assist all members of your family in making wise decisions when it comes to internet usage.
Learn steps you can take to reduce the risks your family faces from online threats, as well as how to secure your home network, especially if working from home.

In this module, you will:

- Discover that cybercriminals target everyone, even home-based users
- Learn how to protect yourself and your family against online fraud
- Explore ways to improve the security of your home network, especially if working from home

New Whitepaper:

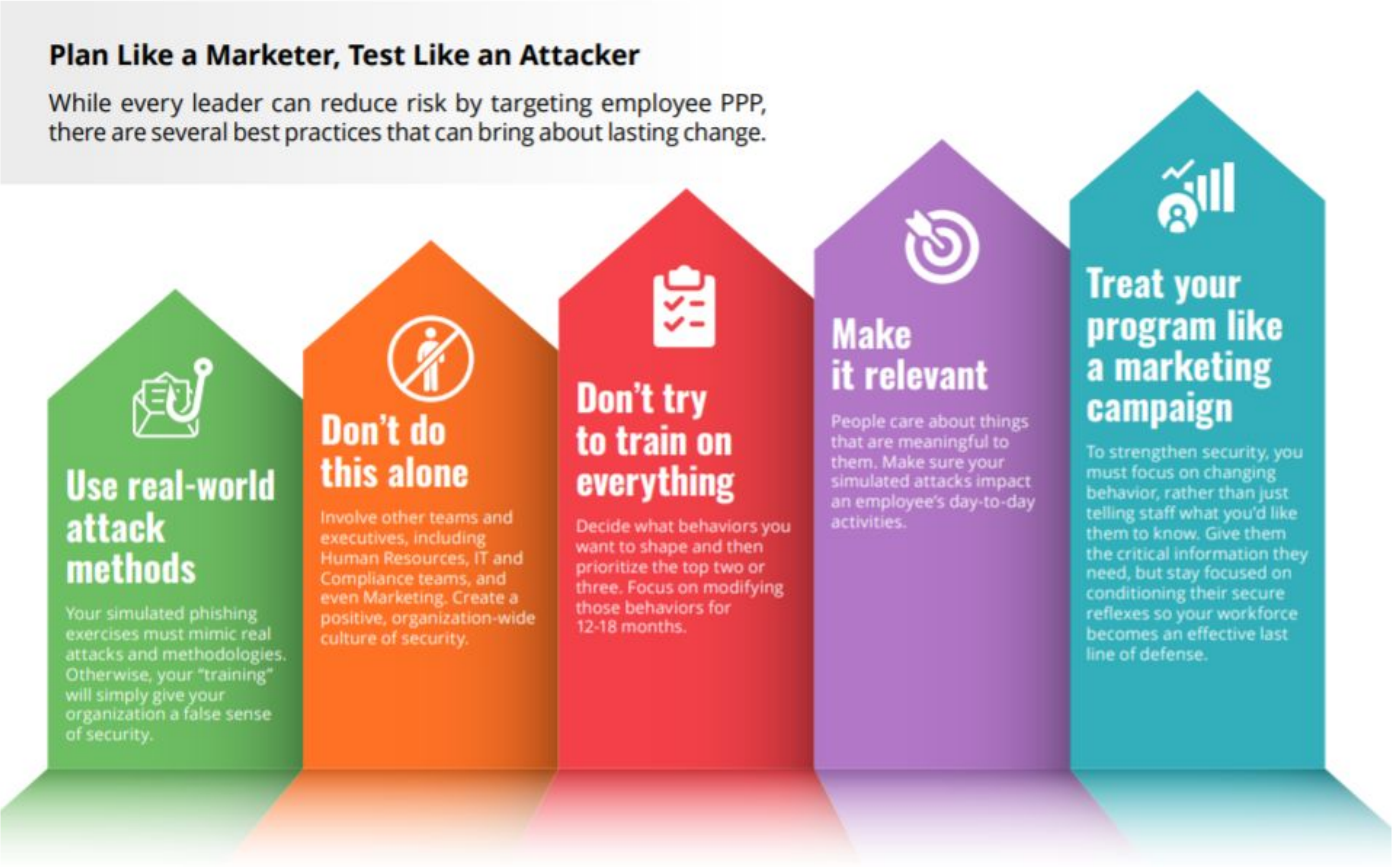
Building an Effective and Comprehensive Security Awareness Program

KnowBe4
Human error. Conquered.

WHITEPAPER

Building an Effective and Comprehensive Security Awareness Program

by Joanna Huisman



Plan Like a Marketer, Test Like an Attacker

While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

Use real-world attack methods

Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

Don't do this alone

Involve other teams and executives, including Human Resources, IT and Compliance teams, and even Marketing. Create a positive, organization-wide culture of security.

Don't try to train on everything

Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

Make it relevant

People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

Treat your program like a marketing campaign

To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their secure reflexes so your workforce becomes an effective last line of defense.

FRESH NEW CONTENT BREAKDOWN 2021…

1,342 Pieces of Education & Training Content

319 Interactive Training Modules

489 Video Modules

23 Mobile-1st Modules

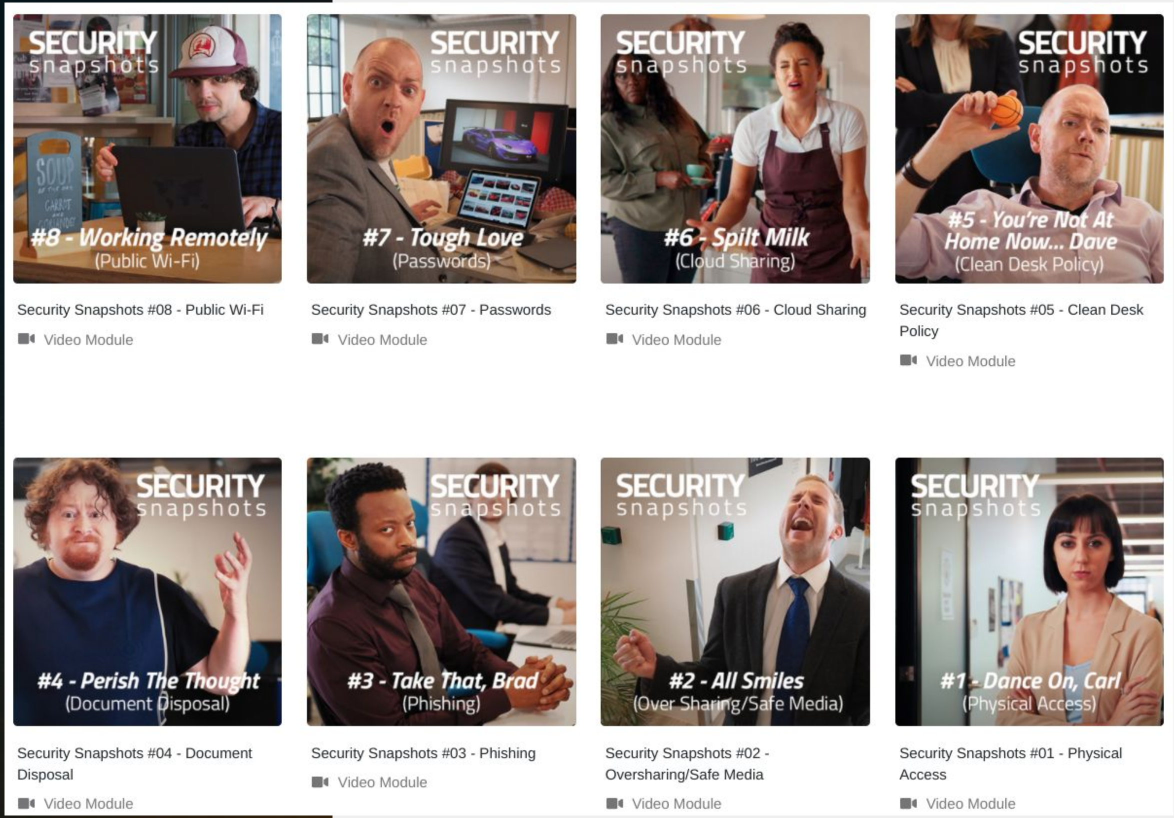
236 Posters & Artwork

248 Newsletters & Security Documents

25 Games

2 Assessments

2 Minute MP4 Videos...



Security Snapshots #08 - Public Wi-Fi
Video Module

Security Snapshots #07 - Passwords
Video Module

Security Snapshots #06 - Cloud Sharing
Video Module

Security Snapshots #05 - Clean Desk Policy
Video Module

Security Snapshots #04 - Document Disposal
Video Module

Security Snapshots #03 - Phishing
Video Module

Security Snapshots #02 - Oversharing/Safe Media
Video Module

Security Snapshots #01 - Physical Access
Video Module

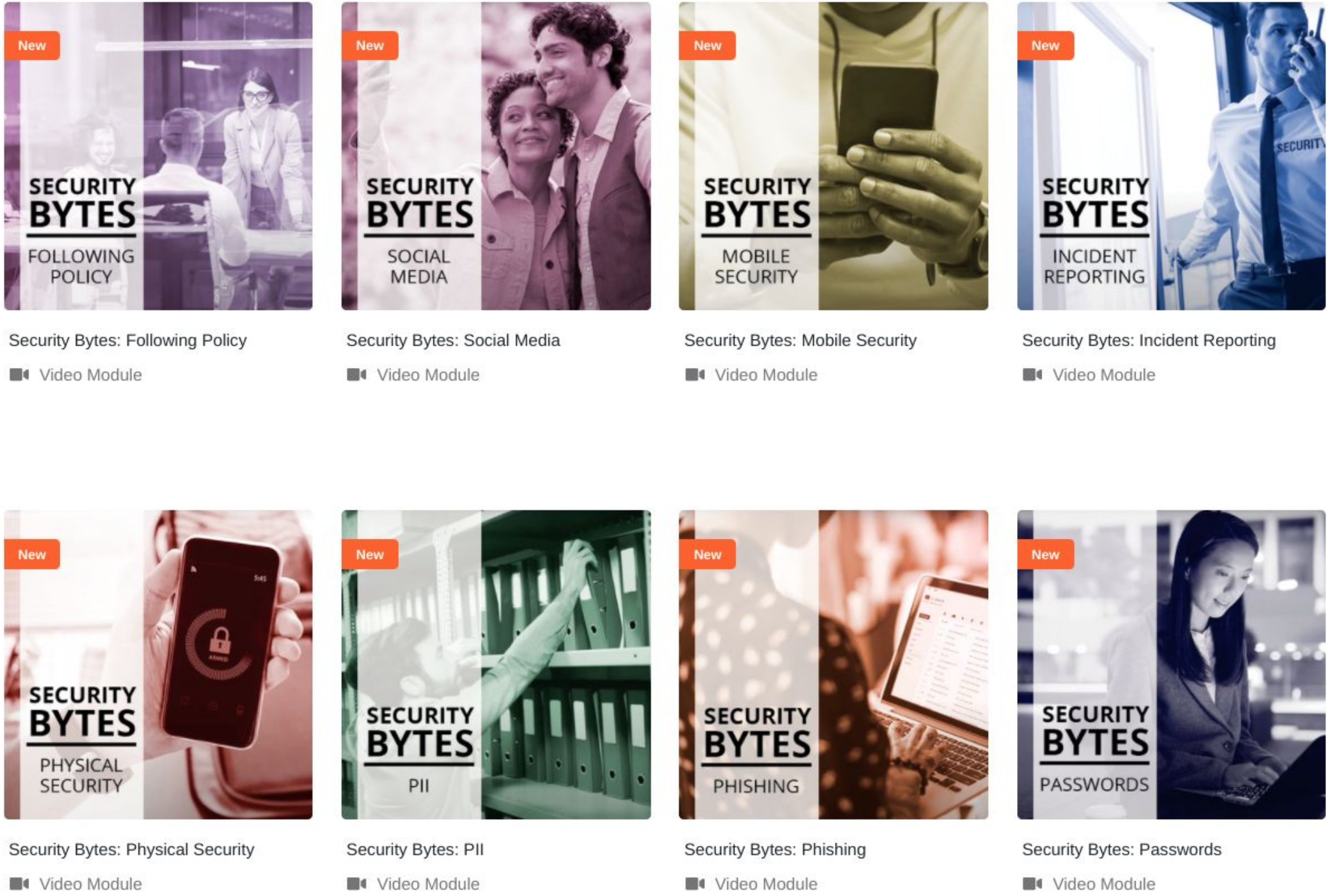
Award Winning Content in the Modstore!

KnowBe4
Human error. Conquered.

New Content

Security Bytes - 1 minute mp4 format

Embed on your Intranet or Video stream site! Expand the message!



Security Bytes: Following Policy
Video Module

Security Bytes: Social Media
Video Module

Security Bytes: Mobile Security
Video Module

Security Bytes: Incident Reporting
Video Module

Security Bytes: Physical Security
Video Module

Security Bytes: PII
Video Module

Security Bytes: Phishing
Video Module

Security Bytes: Passwords
Video Module

New Series September - *Voice on Security...*

Voice on Security: USB Drop

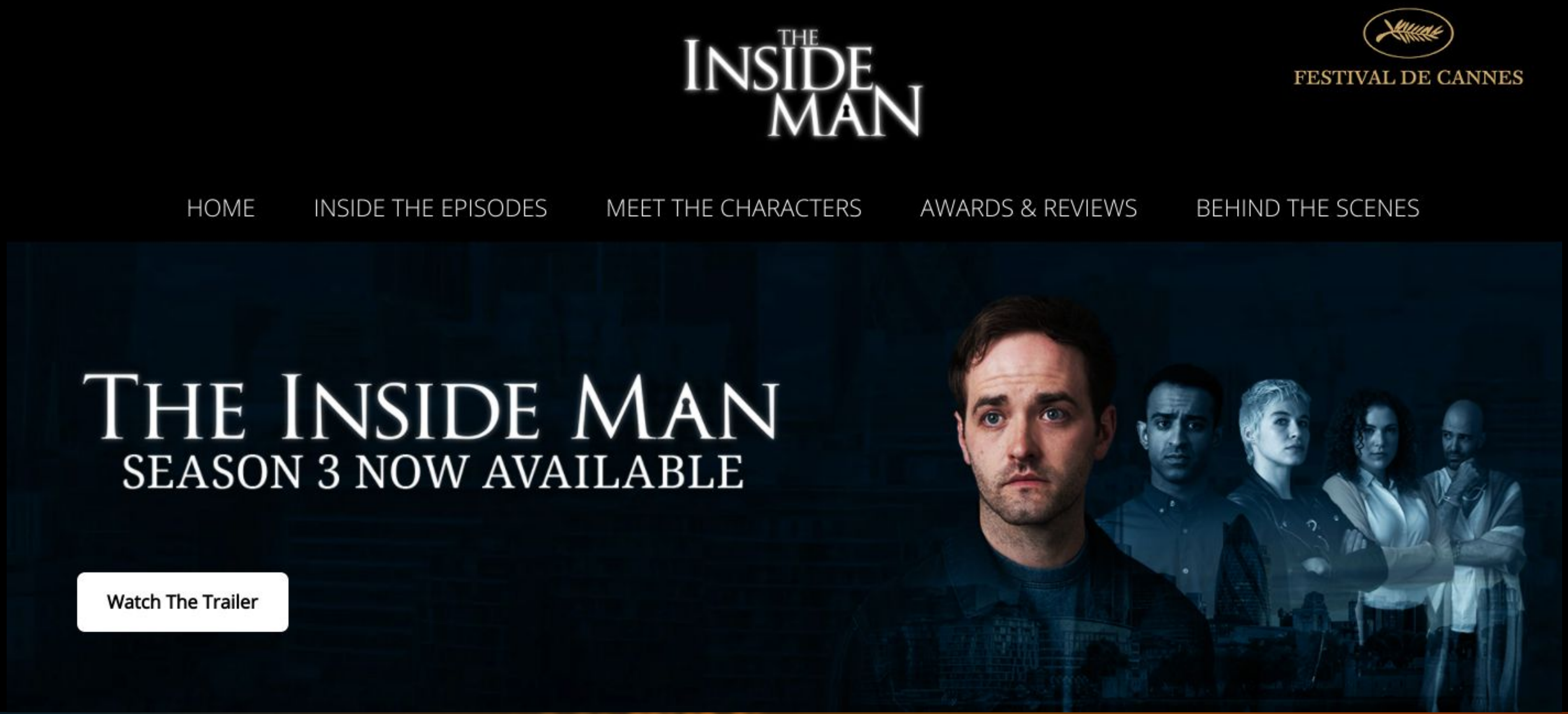
Voice on Security: Piggybacking

Voice on Security: Spear Phishing

Voice on Security: Keep a Clean Desk

From our Partners at The Security Awareness Company - humorous, original, combined with effective training techniques, ranging from 2-3 mins in duration. Now LIVE in the modstore!

https://insideman.knowbe4.com/



Thank You!

KnowBe4
Human error. Conquered.

Know more about KnowBe4.

knowbe4.com
855.566.9234
kathleeng@knowbe4.com