



Building a Security Awareness Program to Help Defend Against Cyber Extortion and Ransomware

by Anna Collard
SVP Content Strategy &
Evangelist KnowBe4 Africa

TABLE OF CONTENTS

Defending Against Cyber Extortion	2
Behavior Design in Security Awareness	2
Motivation.....	3
Ability	3
Prompts.....	4
Building Your Campaign	4
Raising General Awareness	5
Awareness by Top Initial Exploit Causes.....	5
Final Thoughts & Best Practices	7
Appendix: References & Links	8

DEFENDING AGAINST CYBER EXTORTION

Cyber extortion is listed as one of the top worries by cybersecurity professionals throughout the world, with good reason. Ransomware gangs have attacked tens of thousands of organizations from small to very large, brought down hospitals, pipelines, police stations and even entire ports.

At the heart of cyber extortion is the basic idea that if you take something unique and precious from someone, they will pay to have it back. If you discover someone's secret, they will pay you to keep it secret. If they consume all your bandwidth so you cannot conduct business, you will pay them to stop. The microcosmic market of one seller and one desperate buyer, with almost zero risk for the criminal, drives extortion prices and immense profits.



Because of its rise in sophistication and volume, organizations are asked by their cyber insurers, regulators and shareholders to step up their defenses against this threat. Similarly, to other cybersecurity goals, this is not achieved by deploying a shiny “anti-ransomware” tool, but rather through a defense in depth model with multiple layers of control.

Defence-in-Depth

The top initial exploit causes that allow cyber extortionists to compromise devices and environments are (in order of popularity): Social Engineering/Phishing, Unpatched Software, Abuse of Microsoft Remote Desktop Protocol (RDP) and Authentication Attacks.

Building a security culture, or in other words, strengthening your human defense layer and making them aware of how to detect and prevent the initial compromises listed above, is a crucial element in your defense in depth model.

This document outlines an **awareness program** with the objective of strengthening your organization's human layer of defense as a key control in the fight against cyber extortion attacks.

BEHAVIOR DESIGN IN SECURITY AWARENESS

Traditional awareness efforts are based on the belief (or hope) that information leads to action. And although it is an important first step, the limitation with awareness is that “awareness” itself does not automatically result in secure behavior. The goal therefore should be finding effective “behavioral interventions” to bridge the awareness, intention and behavior gap.

Let's look at the problem through the lens of behavior design. BJ Fogg is a social scientist and adjunct professor at Stanford University and referred to as the father of behavior design. [BJ Fogg's behavior design model](#) neatly outlines that **behavior** happens when three things come together at the same time:

Motivation, Ability and a **Prompt**

Motivation

[Fogg's Behavior Model](#) highlights three core motivators: Sensation, Anticipation and Belonging. Each of these has two sides: pleasure/pain, hope/fear, acceptance/rejection. These core motivators apply to everyone; they are central to the human experience.

The list below outlines suggested interventions to trigger people's motivation:

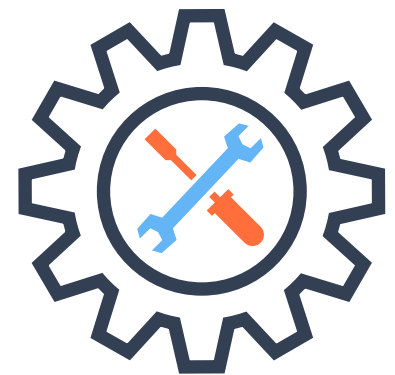
- Tapping into people's emotions by using **visually appealing** content, engaging with **humor** and **story-based** techniques, will activate positive sensations.
 - **Caveat:** Humor is a great technique to grab people's attention, evoke positive emotions and help with memory retention. However, it has to be applied carefully and with a sensitivity to the audience's cultures, or else it can backfire. Also, it should not be used too much, as it could result in the audience not taking the core message seriously enough.
- **Fear** can be a powerful motivator too. But too much of it can result in apathy and needs to be underpinned with the notion that it is **simple to defend**. Show people how to defend themselves. Give them the knowledge and/or tools to feel empowered rather than afraid.
- Using the power of **leadership or celebrity** to tell stories invokes a sense of belonging.
- Making it **personally relevant** by providing information on how to protect family members.
- **Happy people make secure people** – communicate that phishing simulations are not there to trick people, but a training exercise only. Work on building a **trust relationship** between Security and the rest of the community.
- **Recognition** to drive participation. For example, public shout-outs by the CEO if someone reported a significant potential threat.
- **Competitions and rewards** such as phishing tournaments whereby participants can win if they report a specific number of simulated phishes over a certain period of time.



Ability

BJ Fogg says that training people is hard work, and most people resist learning new things. That is just how we are as humans. Giving someone a tool or a resource that makes it easier to do helps break down that barrier. A great example is a password manager. It takes care of desired behavior and simplifies the complexity of having to remember multiple unique passwords. So, when running a ransomware awareness campaign, we need to ask ourselves where are opportunities to provide tools that make it easier for people to stay safe? For example:

- Games to “train” the spotting of phishing attacks in repetitive ways that **convert knowledge into intuitive situational** awareness.
- Equip people with tools such as **phish-alert buttons, password managers, home security**, etc.
- Simple **how-to guides** and short explainer videos or training modules.

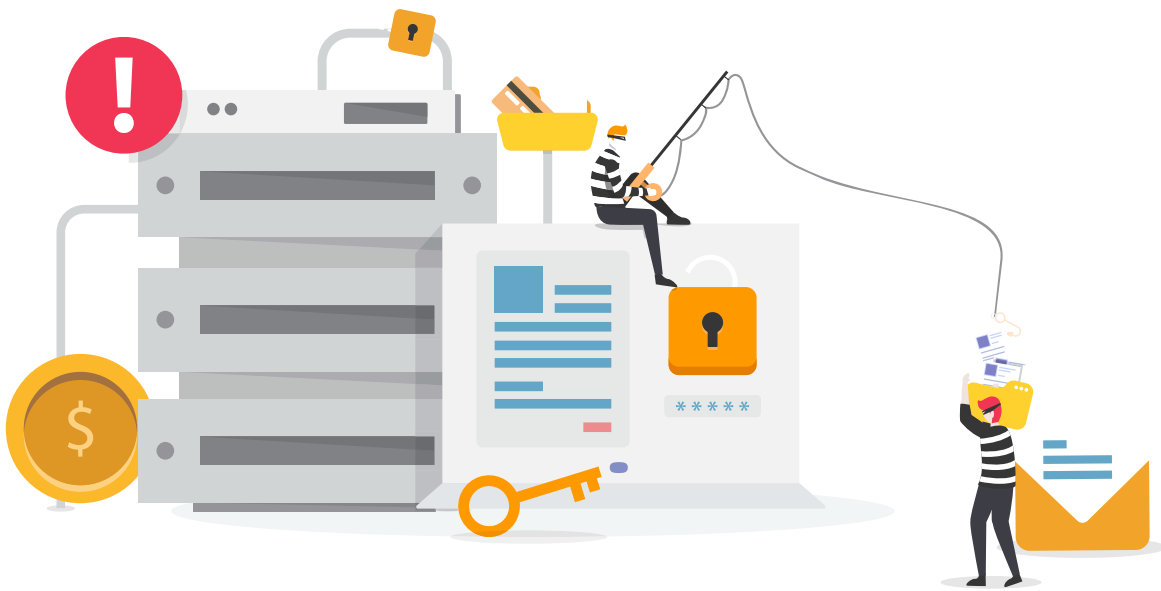


Prompts

The concept of prompt has different names: cue, trigger, call to action, request and so on, and they all have the purpose to remind and tell people to “do it now”. A good example is the password strength meters reminding people to come up with better passwords as and when they create them.

When designing your ransomware awareness campaign, it is important to consider where prompts may be used, i.e.:

- When users join the company, educate them about the extortion threat
- Notes about latest phishing scams
- Phishing detection warnings in user’s email clients (i.e., notes such as “are you sure you can trust this link / attachment?”)



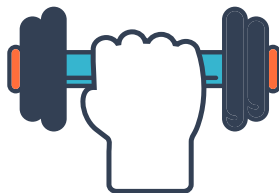
BUILDING YOUR CAMPAIGN

When it is possible to combine the three elements of motivation, ability and prompts, changing behavior is a much more likely outcome than just spreading awareness content and hoping for a result.

MOTIVATION



ABILITY











PROMPTS



Taking the above into account, we suggest the following steps for your cyber extortion awareness campaign:

Raising General Awareness

Goal	Audience	Proposed Intervention	KnowBe4 (and other) Content	Behavior Design Trigger
Sensitize Security and IT Management	IT, Security, Audit, Risk Management	Risk assessment results Scope of problem and predictions of cyber extortion crime Masterclasses	<ul style="list-style-type: none"> • Ransomware Simulator • 5 Things You Need to Know About Ransomware Before It's Too Late • Masterclass on Ransomware prevention 	 
Sensitize VIPs on seriousness of cyber crime	Board VIP Executives	Present risk rating of extortion to business Summary predictions	<ul style="list-style-type: none"> • Present executive summary and results from Ransomware Simulator • Results from Phishing test 	
Sensitize staff about cyber extortion crime and ransomware	All staff	Short education/ awareness on ransomware – mini modules Posters Newsletters	<ul style="list-style-type: none"> • Security Moments Series: Ransomware (2 mins) • Security Snapshots #09 – Ransomware (2 mins) • Poster: Security Moments Series –Ransomware • Ask VIPs to record a message to all staff about the seriousness of this threat • Spot the Phish Game: Foundational (5 mins) 	    



Awareness by Top Initial Exploit Causes









The top initial exploit causes that allow cyber extortionists to compromise devices and environments are (in order of popularity):

1. Social Engineering/Phishing
2. Unpatched Software
3. Abuse of Microsoft Remote Desktop Protocol (RDP)

4. Authentication Attacks

Social engineering is consistently the number one root cause used by ransomware and other malware attacks to gain initial access.

It makes sense therefore to consider raising awareness around these initial attack vectors amongst the groups typically responsible for them.

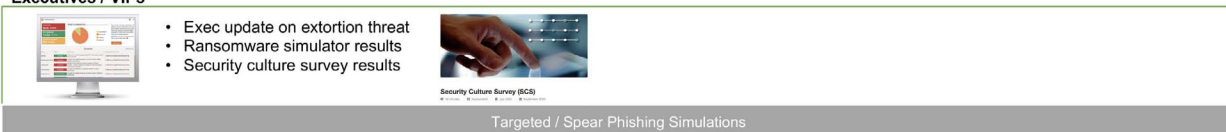
Attack Vector	Audience	Proposed Intervention	KnowBe4 (or other) Content	Behaviour Design Trigger
Social Engineering	All staff	Phishing base training Gamified phishing training to transfer knowledge to intuitive awareness Phishing simulations mimicking typical ransomware phishing techniques	KB4 Training: <ul style="list-style-type: none"> Phishing Foundations (15 mins) Basics of Phishing (5 mins) Spot the Phish Game: Foundational (5 mins) Phish Catcher Game (7 mins) Phishing templates: <ul style="list-style-type: none"> Invoices, calendar invites, payment notification, Delivery notices CV/job applicants (HR) 	   
Unpatched software	IT and	Data-driven defense	<ul style="list-style-type: none"> Masterclass on Data-Driven Defense 	
Microsoft Remote Desktop Protocol (RDP)	IT and	Privileged user training MRDP security guidance	KB4 Training: <ul style="list-style-type: none"> Security Moments Series: Privileged User Access Management (4 mins) Other: <ul style="list-style-type: none"> Microsoft guidelines for securing RDP 	 
Password attacks	IT and	Password policy Understanding multi-factor risks	<ul style="list-style-type: none"> Roger Grimes Password policy Lessons learnt from testing 150 MFA products Provide users with a password-manager tool 	

Final Thoughts & Best Practices

There are some best practices which we have picked up over the years that help when embarking on a security awareness and culture campaign:

1. **Do not manage what you cannot measure.** Create a baseline view of your current awareness status by running a proficiency or security culture assessment and track it every 12 months. This will allow you to showcase improvements. Phish-prone Percentage™ (PPP) can help as a tracking metric, but can be manipulated by changing phish sophistication levels, so this needs to be reported in context.
2. **Involve your executives.** Executive involvement goes beyond sponsorship or budget approval for the campaign. Your executives should be the face of your campaign, people look at what their leaders are doing.
3. **Do not do it alone.** Work with your marketing, internal communications, HR and compliance teams, amongst others, to gain input and approval for your campaign plan.
4. **Combine training with frequent phishing simulations.** Doing quarterly phishing is not enough. Everyone in the company should get a randomly-assigned phish every week (or as often as your corporate culture will tolerate – at least monthly). This gamifies the experience as every email needs to be scrutinized. Create targeted or customized phishing emails for your privileged users.
5. **Remediation training for frequent clickers.** Provide in depth remediation training for frequent clicker-groups, which gets automatically assigned upon a pre-set number of “clicks.” This ensures training is targeted at people who need it.

Executives / VIPs



Targeted / Spear Phishing Simulations

IT & IT Security – Privileged Users



Targeted / Spear Phishing Simulations

All staff



Weekly Randomized Phishing Simulations

Clickers



Suggested cyber extortion awareness campaign plan

By applying BJ Fogg's behavior design model, considering the top exploit causes as well as the best practice points listed above, your cyber extortion awareness campaign becomes more targeted and effective. If you are already a KnowBe4 customer, please speak to your Customer Success Manager for guidance around relevant training modules.

APPENDIX: REFERENCES & LINKS

1. KnowBe4 "Ransomware Hostage Rescue Manual"
<https://info.knowbe4.com/ransomware-hostage-rescue-manual-0>
2. Orange CyberDefense "Protecting Against Cyberextortion"
<https://orangecyberdefense.com/global/white-papers/beating-ransomware/>
3. BJ Fogg Behavior Model
<https://behaviormodel.org/>
4. Free ransomware simulator tool simulating 22 ransomware infection scenarios and 1 cryptomining one to show if a workstation is vulnerable.
<https://www.knowbe4.com/ransomware-simulator>
5. Roger Grimes' webinar "5 Things You Need to Know About Ransomware"
<https://info.knowbe4.com/5-things-you-need-to-know-about-ransomware>
6. Roger Grimes' webinar on defending against ransomware
<https://info.knowbe4.com/ransomware-master-class>
7. Microsoft guidelines on securing remote desktop adoption
<https://www.google.com/url?q=https://www.microsoft.com/security/blog/2020/04/16/security-guidance-remote-desktop-adoption/&sa=D&source=docs&ust=1638361687417000&u sg=AOvVaw1vUECqF-O0n9FEwl89cieL>
8. Roger Grimes' webinar on data-driven defense
<https://info.knowbe4.com/data-driven-defense-master-class>
9. Roger Grimes' webinar on multi-factor authentication
<https://info.knowbe4.com/hacking-150-mfa-products>
10. Roger Grimes' webinar on password policy
<https://www.youtube.com/watch?v=ByuUdsLIYC8>



Additional Resources



Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test



Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization



Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click



Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do



Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com