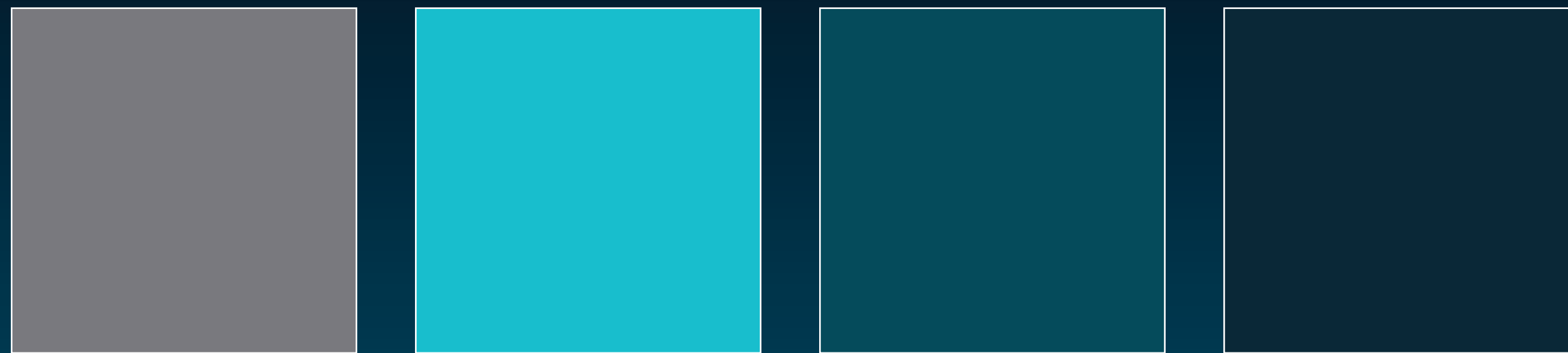


# KEEPING IT REAL

The concept behind Keeping It Real is to create a campaign that spreads awareness of the general issue of cybersecurity by educating the masses on the different types of cyberattacks that exist on the web, and the vitality of having strong security put in place to avoid having one's valuable data compromised. This not only includes important files on one's computer or any other digital device, but also one's finances as well as their personal identity and general welfare.



## DELIVERABLE 1 | AD FLIERS

**I WANT YOU!**

**PROTECT YOUR CHILDREN.**  
Children are 5x more susceptible to becoming victims of identity theft than adults.

KEEPING IT REAL  
keepingitreal.org

**NOTHING IS PRIVATE.**

**ALWAYS BE ALERT.**  
Be careful of where you browse. Clearing your history doesn't cover your tracks.

KEEPING IT REAL  
keepingitreal.org

**ARE YOU SECURE?**

**YOU'RE BEING WATCHED.**  
Check your network's security first and foremost. Your online data can be intercepted at any given moment.

KEEPING IT REAL  
keepingitreal.org

**KEEPING IT REAL**

**USER GUIDE FOR INTERNET SAFETY**

## DELIVERABLE 2 | WEBSITE

KEEPING IT REAL

MISSION RESOURCES TESTIMONIALS FAQ CONTACT

**KEEPING IT REAL**

We are committed to ensuring a safe space on the worldwide web, as your internet safety is as vital as your physical and financial safety. Our number one priority is to create awareness towards the importance of internet safety through providing courses that explore different types of cyberattacks, along with the harm that they can cause and how to safely stay out of harm's way.

Learn More

"Keeping It Real has really helped me gain vigilance towards surfing the web in terms of checking to see if the websites I visit have HTTPS instead of HTTP before the URL, since the difference between the two is literally night and day."  
— K. F.

"Thanks to Keeping It Real, my family has increased security measures for both our network and all our devices through adding extra protective layers, in addition to backing up our data more regularly."  
— J. S.

"Keeping It Real is literally a lifesaver. I'm way more prompt with keeping my devices up to date, along with checking my computer's antivirus software more frequently to see if it's doing its job keeping the bad guys out."  
— M. P.

Join our newsletter!

example@gmail.com Country / Territory

SUBSCRIBE

RESOURCES WHAT WE DO TESTIMONIALS FAQ CONTACT US (781) 252-7495 info@keepingitreal.com

KEEPING IT REAL  
© 2022 KEEPING IT REAL. ALL RIGHTS RESERVED. CONNECT WITH US

PRIVACY DO NOT SELL MY PERSONAL INFORMATION TERMS

KEEPING IT REAL

MISSION RESOURCES TESTIMONIALS FAQ CONTACT

**OUR MISSION**

Our mission here at Keeping It Real is to help create the proper awareness towards staying safe on the internet, while at the same time expose the unprecedented dangers that exist and how to safely navigate around them without becoming a potential target or victim. Cyberattacks typically occurs nearly once every 39 seconds, and claim more than 800,000 victims worldwide on an annual basis.

Aside from the physical damage caused by cyberattacks being detrimental, so can one's psychological effects, which can persist for weeks, if not months. Psychological impacts from cybercrime include an increase in anxiety, secondary victimization, depression, a sense of helplessness, fear and perceived risk, in addition to a lack of trust and loss of autonomy, which often are outcomes of a sense of violation.

It is our duty to empower people through providing successful strategies and skill sets on ways to be safe on the internet, which range from protecting your digital security all the way to identifying fraud and more. We work closely with the Digital Forensics Corporation to monitor cyberthreats and handle data breach incidents nationwide.

Join our newsletter!

example@gmail.com Country / Territory

SUBSCRIBE

RESOURCES WHAT WE DO TESTIMONIALS FAQ CONTACT US (781) 252-7495 info@keepingitreal.com

KEEPING IT REAL  
© 2022 KEEPING IT REAL. ALL RIGHTS RESERVED. CONNECT WITH US

PRIVACY DO NOT SELL MY PERSONAL INFORMATION TERMS

KEEPING IT REAL

MISSION RESOURCES TESTIMONIALS FAQ CONTACT

**RESOURCES**

Download a PDF of Local & National Resources

**INTERACTIVE GAMES**

**INFORMATIVE VIDEOS**

**PARENTAL RESOURCES**

Join our newsletter!

example@gmail.com Country / Territory

SUBSCRIBE

RESOURCES WHAT WE DO TESTIMONIALS FAQ CONTACT US (781) 252-7495 info@keepingitreal.com

KEEPING IT REAL  
© 2022 KEEPING IT REAL. ALL RIGHTS RESERVED. CONNECT WITH US

PRIVACY DO NOT SELL MY PERSONAL INFORMATION TERMS

## DELIVERABLE 3 | BROCHURE

**THE RISE OF CYBERCRIME**

Cyberattacks occur nearly once every 39 seconds and claim more than 800,000 victims worldwide on an annual basis. Such attacks include malware and phishing attacks, denial of service threats, ransomware, insider threats, and more. The rates of cybercrime have tripled since the start of the pandemic, and have affected the security of more than 80% of businesses worldwide. This is due to the limited capabilities that authorities have towards monitoring cyberattacks since cybercrime takes place virtually. Ransomware has been a significant threat to businesses on a global scale, and according to cybersecurity statistics, more than half of cyberattacks are committed through ransomware attacks. In addition, healthcare databases are the most vulnerable to cyberattacks due to their level of importance towards businesses and their possession of high monetary information and intelligence value to cybercriminals. The three major types of ransomware include crypto ransomware, which encrypts system files, locker ransomware which locks a device's screen until a ransom is paid, and wiper ransomware which completely wipes files stored on a hard drive. With the rising trends in cryptocurrency, it has been suggested by experts that ransomware will become the easiest form of cybercrime in the following year, expected to affect a total of more than 8 million users or 10% of all internet users.

**WHY YOU SHOULD CARE**

Cybercrime can affect any individual or business at any given moment. It is imperative to care about cybercrime in order to keep all your devices and data assets safely protected and avoid becoming a potential victim to a malicious software attack known as a cyberattack, or any other cyberthreat. It is critically imperative to care if you are a parent of a young child or children. Physical damage from cyberattacks can include security breaches in business all the way to theft and exposure of important confidential personal data such as Social Security Numbers, bank account information, addresses and more.

Aside from the physical damage caused by cyberattacks being detrimental, so can the psychological effects on oneself, which can persist for weeks, if not months. Psychological impacts from cybercrime include increased anxiety, secondary victimization, depression, a sense of helplessness, fear and perceived risk, in addition to a lack of trust and loss of autonomy, which often are outcomes of a sense of violation.