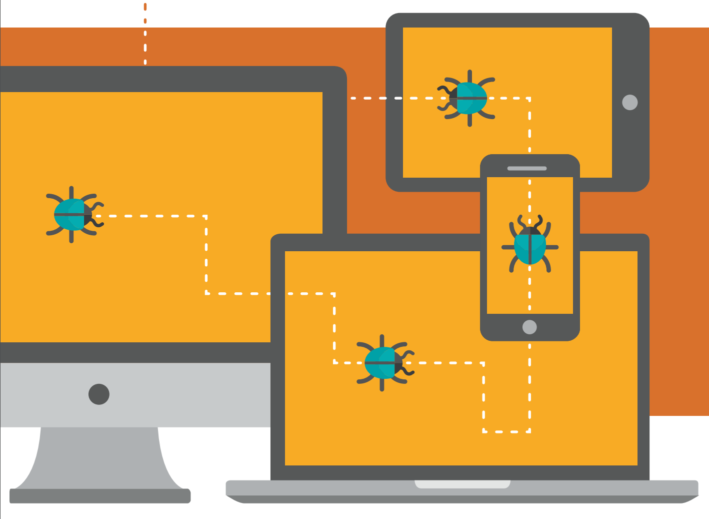
Dynamic Campus

Ransomware on Campus:

How to Protect Yourself

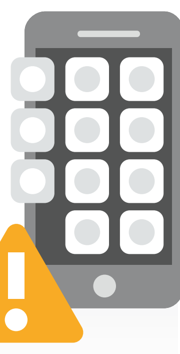
1 IN 10

College and university networks have a high degree of susceptibility to ransomware, making higher education the #1 target for these attacks[1].



RANSOMWARE CAN INFECT YOUR COMPUTER, PHONE OR ANY CONNECTED DEVICE, AND PRESENTS A SERIOUS RISK TO YOUR DEVICE AND DATA!

How ransomware spreads



Ransomware viruses typically spread via:

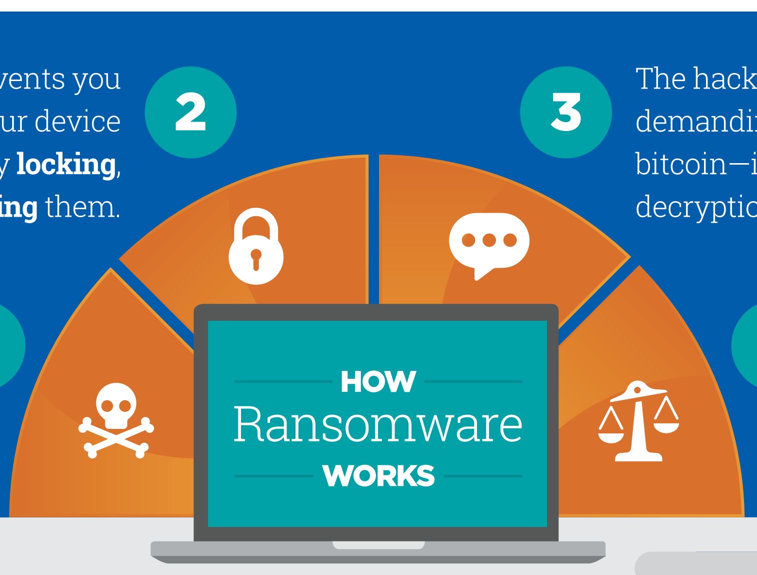
EMAIL

93% of phishing emails today contain some type of ransomware. These emails include fake:

- ATTACHMENTS
- LINKS
- FORMS
- BUTTONS

MOBILE APPS

Third-party apps meant to look like free versions of paid apps. These are usually found on websites or app stores that are not maintained by Apple or Google.



1 The ransomware virus infects your PC or mobile device via an e-mail or app.

2 Once in place, it prevents you from accessing your device and/or data by **locking**, **blocking** or **encrypting** them.

3 The hackers contact you directly, demanding money—in untraceable bitcoin—in exchange for a decryption key they send you.

4 You decide whether to pay the ransom or not, and hope the hackers are true to their word.

Unfortunately, victims that choose to pay are placed on a "known payer" list shared by hackers. This increases the likelihood of future attacks, and the ransom amount requested grows.

How to avoid ransomware attacks

DON'T FALL FOR PHISHING EMAILS, TEXTS OR POSTS.
If you get an email, text or a social media message with an odd request, link or attachment, **don't do anything**.

KEEP YOUR COMPUTER, PHONE AND APPS UP TO DATE.
This fixes any potential vulnerabilities before hackers can take advantage of them.

ONLY DOWNLOAD MOBILE APPS FROM AUTHORIZED SITES.
Apple's App Store and Google's Google Play are the only authorized app download locations. Downloading from anywhere else is a dangerous gamble.

BACK YOUR STUFF UP REGULARLY.
Set your computer and phone to back up your data automatically to the cloud or a storage device every day. If hackers manage to hold your data hostage, you've got the upper hand!

What to do if you're a victim

DO NOT
respond or negotiate

if you receive a ransom note from a potential hacker by email, phone, text or social media.

DO
contact our IT support team.

We will work with you to determine the proper course of action based on your situation.

[1] "The Rising Face of Cyber Crime: Ransomware" Bitsight Insights, 2017