BACK TO SCHOOL
CRASH COURSE IN CYBER SECURITY

In today's digital world, college students regularly use smart devices to complete assignments, communicate with professors and peers, as well as surf the web. In fact, 18-44 -year-olds are significantly more likely to use their tablet or smart phone for homework than any other age group, according to Trend Micro's 2016 Global Consumer Security Survey. As part of preparation for the fall semester, it's important to understand how to secure your devices.

GRADUATION
After graduation students determine the right devices for success

The average college student owns
7 TECH DEVICES

18-44 years old use a tablet/smart phone for homework, as well as photo/video editing

92% of 18-29-year-olds own a smart phone, according to Pew Research Center

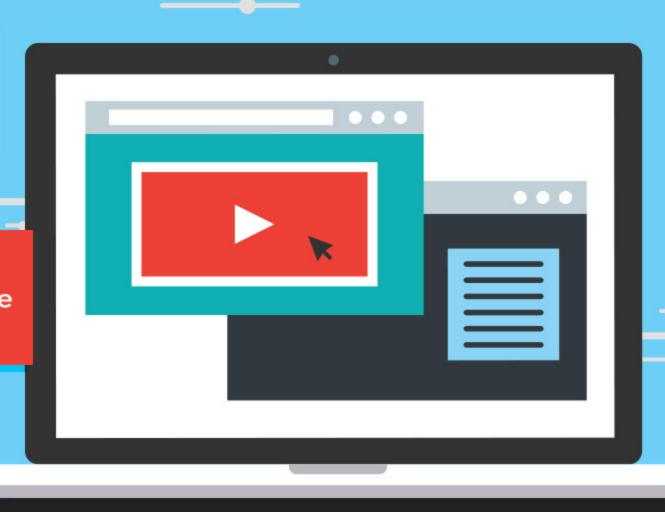**1 IN 3** respondents have heard the term ransomware before

FIRST DAY OF CLASS
Some quick stats to provide an overview of why digital security is important

65% of individuals have experienced a virus or malware

45% of individuals have clicked on malicious URLs or went to unknown websites

19% of people are very concerned about the threat of ransomware

How to get an A in Cybersecurity

Easy steps to mitigate the chances of falling victim to a cyberattack

Shopping for the right software
- Effective performance and price are the top two factors people consider when shopping for security software
- Understand the features and protections the software offers, how it will affect your device and whether or not it's sold by a credible vendor

Change your passwords
- Using the same password for everything is akin to rolling out a welcome mat for cybercriminals
- Your password should not only be different for you various account, but each one should be complex and frequently changed

Back up your files
- Use the 3-2-1 rule for backing up and preserving your information
- If you're backing something up, you should have:
  o At least **3** copies
  o In **2** different formats
  o With **1** of those copies off-site

Familiarize yourself with attacks that are most common
- 2016 witnessed a 752 percent increase in ransomware families – threat actors are getting smarter about their attacks, so you should be learning more about protecting yourself.

Don't open suspicious links or email attachments
- More than 61 percent of malware attacks are delivered via email attachments and malicious websites

Don't leave devices unattended – physical safety
- Once again, keeping a watchful eye on your devices will ensure they don't end up lost or stolen, along with the rest of your personal information, photos and documents.

Update your software and devices
- Once you've researched and installed the best security for you, be sure to consistently update the software to ensure the utmost protection
- Similarly, you should be downloading the most recent updates for each individual device. These updates often entail security patches that are crucial to your protection.

$$a^2 + b^2 = c^2$$

BROKE COLLEGE KIDS CAN'T AFFORD TO PAY THE RANSOM!

DON'T PAY THE RANSOM!
90% of respondents said they wouldn't pay the ransom if prompted to do so. There's never a guarantee you'll get your information back, so not only will your information be compromised, but you'll also be out several hundred dollars.

28% of people are likely to contact an IT specialist in the event of a cyberattack.

LAST MINUTE TIPS BEFORE THE TEST

1. Use a password manager to keep up with your various passwords.

2. Install Trend Micro Maximum Security with protection for up to 10 devices. One software for your tablet, laptop, smartphones and desktop computer? Talk about cost effective, consistent and reliable security!

3. Know what to look for. Even the most genuine looking email could be a phishing scam. Ensure any attachment you open or link you click on is coming from a reliable source and make sure your security software is monitoring for these illegitimate attack methods.

TREND MICRO