Preventing Data Breaches and Identity Theft

Sun Ow, Director of Sales – BankMobile
Today’s Agenda

1) Cybercrime environment
2) Who are the targets?
3) Why do they do it?
4) How are they attacking?
5) What’s the cost?
6) What can higher education professionals be doing?
Organizations lost $301 per employee due to endpoint attacks in 2017
Cyber Security Trends

**RANSOMWARE**
Prepare to be exploited in 2016 as criminal gangs rush to make the most of this lucrative ‘business’.

165% RISE

**RISE OF THE BOTS**
IOT devices that can lock, monitor or have access to your data will become prevalent, bringing a new breed of vulnerabilities with them.

50 BILLION DEVICES

**MOBILE MALWARE**
A steep rise in malicious apps will threaten all mobile device users and their data as the entry barriers to app development come down.

20 MILLION BAD APPS

**CLOUD DATA**
The cloud industry is forecast to grow by 18.4% - while most security policies are still reliant upon simple SSL encryption.

4.6 BILLION CLOUD USERS

**500 Gbps DDOS ATTACKS**

**HACTIVISM**
More people will take justice into their own hands - weather through leaking confidential data or unleashing DDOS attacks against their perceived enemies.
Who is a Target?

1 MILLION+ VICTIMS A DAY
EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES

SHOCKING SCALE: NUMBER OF VICTIMS

50,000 VICTIMS EVERY HOUR
820 VICTIMS EVERY MINUTE
14 VICTIMS EVERY SECOND

7/10 69%
69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime.

589 MILLION
Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world.

65%
Among all cybercrime victims surveyed, nearly two thirds have fallen prey in the past 12 months alone - a total of 431m adults in 24 countries.

431 MILLION
The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m) or Western Europe (400m).

©2018 BankMobile Technologies, a wholly owned subsidiary of Customers Bank. All Rights Reserved
Distribution of Targets

March 2018

- Individual: 22.4%
- Multiple Industries: 15.3%
- Public administration and defence, compulsory social security: 11.2%
- Financial and insurance activities: 9.2%
- Human health and social work activities: 7.1%
- Education: 6.1%
- Transportation and storage: 4.1%
- Arts entertainment and recreation: 4.1%
- Electricity, gas steam and air conditioning supply: 4.1%
- Other service activities: 3.1%
- Manufacturing: 2.0%
- Wholesale and retail trade: 2.0%
- Accommodation and food service activities: 1.0%
- Information and communication: 1.0%
- Water supply, sewerage waste management: 1.0%
- Professional scientific and technical activities: 1.0%
- Fintech: 0.0%

hackmageddon.com
Why is Higher Education a Target?

- **Social Security numbers**, bank accounts, credit cards, health information and students’ parents’ information are hot items for hackers.

- **Breaches at universities were up 164%** in the first 6 months of 2017.

- **Securing data poses an enormous challenge** as the cycle of students, alumni, and faculty constantly changes.

- **Universities and colleges can have multiple networks and systems** that are difficult to integrate or you may use 3\textsuperscript{rd} party contractors.

- **Home-grown/ In-house programs could have been developed years ago** and are now outdated, making them difficult to modify and upgrade and difficult to secure.
How Are They Attacking?

### Attack Vectors

- **Malware/PoS Malware**: 39.8%
- **Unknown**: 20.4%
- **Account Hijacking**: 18.4%
- **Targeted Attack**: 16.3%
- **DDoS**: 4.1%
- **Brute Force**: 1.0%

March 2018

[Source: hackmageddon.com]
Why Do They Do It?

Motivations Behind Attacks
March 2018

- Cyber Crime: 76.5%
- Cyber Espionage: 19.4%
- Cyber Warfare: 3.1%
- Hacktivism: 1.0%

hackmageddon.com
Cybersecurity Plans: WHAT CAN YOU DO?
The Basics

• Who has access? (Faculty, Staff, Work-Study students.  Do you have two-factor authentication?)

• What is on the network? (do you maintain different networks for more sensitive info?)

• Where is the data? (where are your data servers? Where do you keep back-up data files?)

• What has the most value?
What your campus can do

1. Develop, implement and maintain a comprehensive information security program with written policies and regular training on prevention
2. Employ an IT security officer responsible for executing the program
3. Hire an independent expert to conduct a security assessment
4. Maintain and support data security software on the company's network
5. Segregate the Social Security data from the rest of the network
6. Take steps to control network access, including password rotation policies and two-factor authentication.
7. BACKUP Your Data Daily and keep it in a safe place away from your main office, if possible.
Cybersecurity Tips – Share With Your Teams and Students!

• Realize that you and your teams are an attractive target to hackers. Don’t ever say “It won’t happen to me.”

• Practice good password management. Use a strong mix of characters, and don’t use the same password for multiple sites. Don’t share your password with others, don’t write it down, and definitely don’t write it on a post-it note attached to your monitor.

• Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you’re gone.

• If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well and encrypt it.

• Never click on a link in an email -if it’s unexpected or suspicious for any reason, just delete the email. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.

©2018 BankMobile Technologies, a wholly owned subsidiary of Customers Bank. All Rights Reserved
Cybersecurity Tips – Share With Your Teams and Students!

• **Back up your data regularly**, and make sure your anti-virus software and operating system is always up to date. Set those programs to update automatically.

• **Be conscious of what you plug in to your computer.** Malware can be spread through infected flash drives, external hard drives, and even smartphones.

• **Watch what you’re sharing on social networks.** Criminals can befriend you and easily gain access to a shocking amount of information—where you go to school, where you work, when you’re on vacation—that could help them gain access to more valuable data.
Cybersecurity Tips – Share With Your Teams & Students

• **Offline, be wary of social engineering**, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it’s okay to say no.

• **Do not** open shared documents that you are not expecting to receive.

• **Be cautious, slow down**. Criminals count on your being too busy or distracted to really look at that email or website.
Preventing Personal Identity Theft

• **Review credit transactions and bank account balances on a regular basis.** Report any discrepancies or suspicious activity to your credit card company and file a dispute & add a Fraud Alert.

• **Monitor your credit score and check your full credit report regularly.** Understanding your report can help you identify fraudulent activity or errors that could hurt your credit score. (use: www.annualcreditreport.com)

• **Set up online account alerts with your bank.** Track account activity real-time to help you to stay in the know about your finances and head off fraudulent activity.
Preventing Personal Identity Theft

• Don’t give out your personal or account information over the phone or through email. The IRS or Direct Loan Servicer will never contact you and ask for social security number or other confidential information.

• Never use public WiFi or public computers for online banking. This could leave your personal or account information susceptible to a wide range of attacks.

• Update your phone Apps for bug fixes.
Fraud Detection

- Look for FAFSA applications with the same student address, phone, or email.
- Do a verification with a notarized document, such as a driver’s license or two pieces of recent bills with the student’s address and than look up the Notary by their license to make sure that it’s a valid Notary
- Work with your IT department to do a query for you.
- Review where the fraudulent emails and calls are incoming from (i.e. the same phone or webserver).
- Some fraudsters are also applying as transfers from multiple schools and you can ask for transcripts directly from those schools, including high school academic transcripts to be sent directly to your school.
Recap: Here are some of the steps to protect your Campus

1. Develop, implement and maintain a comprehensive information security program with written policies and regular training on prevention
2. Employ an IT security officer responsible for executing the program
3. Hire an independent expert to conduct a security assessment
4. Maintain and support data security software on the company's network
5. Segregate the Social Security data from the rest of the network
6. Take steps to control network access, including password rotation policies and two-factor authentication.
Recap

• Prevention
  – Solutions, policies and procedures need to be identified to reduce the risk of attacks.

• Resolutions
  – In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat.

• Restitutions
  – Institutions need to be prepared to address the repercussions of a security threat with their employees and students to ensure that any loss of trust is minimal and short-lived.
THANK YOU!

Sun Ow – Director of Sales, BankMobile
Email: sow@bankmobile.com
Phone: 415-525-6884