A.M. Edition

Insights For Higher Education

Join Adam McDonald, TouchNet president, as he discusses various industry topics, shares insights and spotlights new trends to make sure you're up to date on all things campus commerce and credentials related!

Welcome to the A.M. Edition

Staying Two Factors Ahead of Online Fraud

November 20, 2018

Our COMTEC users conference just ended, and one frequently discussed topic was the growing concern and continued need for campuswide data protection and cybersecurity. Hackers and con men are nothing new. But the more our lives center around online channels the more scammers and phishers switch to online tactics to perpetrate fraud.

In 2017, security expert Symantec estimated there were roughly 135 million attempted phishing attacks every day. According to EdTech, in higher ed, schools are successfully educating users and raising awareness to avoid security breaches, which has reduced the number of successful attacks. However, new scams are always on the horizon, and schools must take every opportunity to prevent these expensive and destructive crimes.

This past August, the government warned institutions of higher education about a new wave of phishing scams aimed at students. Timed during peak Federal Student Aid (FSA) refund distribution periods, these attacks tricked students into providing personal information. The attackers then used that data to divert funds from student direct deposit accounts into their own illegal accounts.

In its phishing alert memo, the Department of Education advised schools to switch from traditional Single Sign On (SSO) protocols to more secure methods, such as two-factor (2FA) or multi-factor (MFA) authentication. Such methods benefit schools and students alike; the student's account is protected from funds being illegally diverted, and the school has an added layer of assurance that any changes made are executed by the lawful account owner

If you're interested in implementing 2FA on your campus, look at places where sensitive data or payment data is captured, entered or stored, such as payment methods, refund details or contact information. By requiring an additional, newly generated code sent to a separate device to be entered before the account is updated, fraudulent attempts to access the account are averted.

There is no way to know what threats lie ahead, but it's a given that vigilance, ongoing preparation, and education will be key to minimizing their impact.

Thanks for reading,

Adam McDonald
adam.mcdonald@touchnet.com

A.M. Edition

2018

Happy Holidays to You From TouchNet
December 11, 2018

Staying Two Factors Ahead of Online Fraud
November 20, 2018

Are You Ready for the NFC Wave?
October 16, 2018

Acquirer: Partner or Problem?
September 11, 2018

Let's Talk About Omnichannel Payments
August 8, 2018

Good Morning, I'm Adam McDonald.
July 10, 2018

Toughey Talks Archives:

2018
2017
2016
2015

Stay In the Know!

✉ Subscribe Now!

Subscribe to our email newsletters