BANKING & ACCOUNTING OPERATIONS NEWSLETTER #11 JULY 2019

A DIFFERENT KIND OF SOCIAL SECURITY - PROTECTING YOUR BUSINESS FROM SOCIAL ENGINEERING FRAUD

Banking & Accounting Operations team attends webcasts hosted by UW's bank partners on a regular basis. Recently, BAO attended a webcast hosted by Bank of America titled, "A Different Kind of Social Security – Protecting Your Business from Social Engineering Fraud". This webcast covered the past, current, and future state of cyber fraud occurring around the world.

What is Social Engineering?

Social engineering is the art of manipulating people so they give up confidential information. Social engineering attacks happen at work, home, in person, and on mobile devices. It takes advantage of human weaknesses.

Evolving Cyber Crime Trends

- In 1989, the first cyber-attack was launched, since then, the tactics and intent have become more sophisticated and malicious. For example, in 2018, FBI reported $12B+ in losses due to Business Email Compromises (BEC) between Oct. 2013 – May 2018.

- Business Email Compromises (BEC) – One of the biggest ways fraudsters are attacking financial institutions around the world. For example, a fraudster hacking into your email account to request funds from vendor to a different bank account, or sending phishing emails to obtain financial information. These types of activities are only increasing and techniques are changing constantly.

- Education Services is listed as one of the top 7 industries as a target for cybercrime.

Associated Finance Professional (AFP) 2018 Fraud Study

- In 2018, a record-setting **82%** of financial professionals report that their organizations experience attempted and/or actual payments fraud in 2018
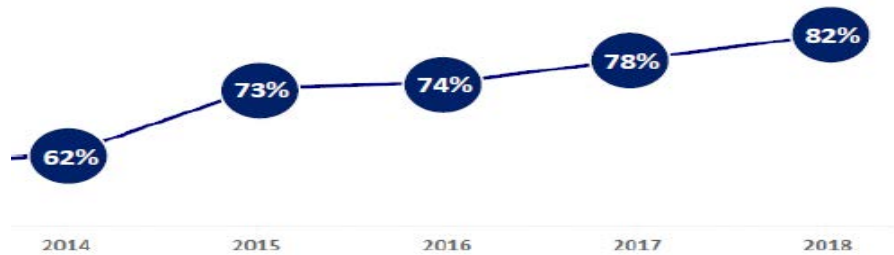
- Check fraud is still the highest payment fraud, however, it has been on a decline. But the decline has been offset by the increase in payment fraud via WIRE and ACH
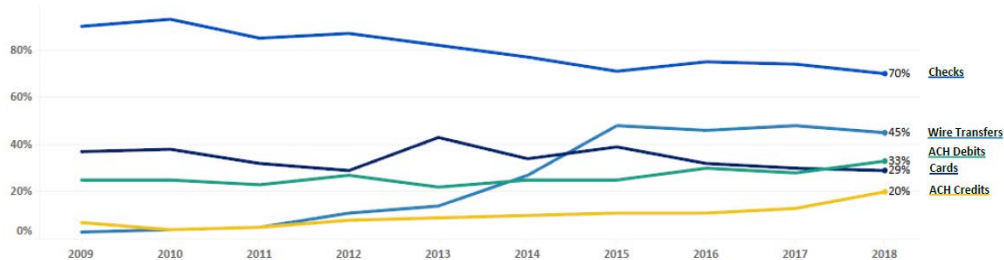
Security Best Practices

- Never reply to an email requesting a change in payment instructions
    - o **Beware**: Sudden changes, or urgent requests should bring up a red flag.
    - o **Validate**: Don't reply to the email right away, instead call the company or start a new email. To verify, ask for old invoice #s or dollar amounts, and request banking instructions on company or bank letterhead.
    - o **Be Pro-Active**: Reach out to vendors to clarify their process of validating change of payment instructions, revisit vendor contracts and identify liability clause.
    - o **Create Process:** Dual approval process, develop procedures for non-standard payment request, empower a slowdown process without pressure.
- 89% of organizations have experienced a data breach, of which almost 2/3 are the direct result of employee error

- o Ongoing education is critical to success.
- o Train before any new employee talks on the phone or accesses the internet.

If you would like to download the presentation deck of this webcast, please visit BAO's Newsletter website below. The slide deck will be under Newsletter #11:

BAO Newsletters

DID YOU KNOW

- BAO provides a monthly report to campus on cash/check deposits that post on UW's main operating account. To review your deposits, please click here.

- 2017–2019 biennium year has closed, however, Cash Transmittals (CTs) and other account entries can be submitted in July. For more information about deadlines related to accounting entries, click here.

- For additional contact information for Banking & Accounting Operations, please click here.

BAO Update

BAO and Office of Merchant Services recently participated in an Escape Room as a team-building activity. Glad to say we successfully escaped the room with 1 minute and 35 seconds to spare!

BAO is committed to providing campus departments with high-quality customer services. Please send your feedback or suggestions to bankrec@uw.edu to help us improve our services.