Cybersecurity

Pandemic Edition

How Cyber Adapted (Education)

- Pandemic created new (but not really new) issues with business continuity. (zoom)

- Remote learning adoption (k-12 to colleges)

- Issues with remote learning (internet, technology gaps, motivation)

- Trial and error and expectations

How Did Cyber adapt? Not well...

What we thought students were doing...

What they were actually doing...

What did we learn…?

- Take away 1: Students need to be highly motivated to succeed in a remote learning environment
- Take away 2: Instructors need more prep time for virtualized courses with less resources available for both student and instructors
- Take away 3: Programs who can adapt quickly to changes were the most successful
- Cyber was a mostly successful program going virtual with a few exceptions
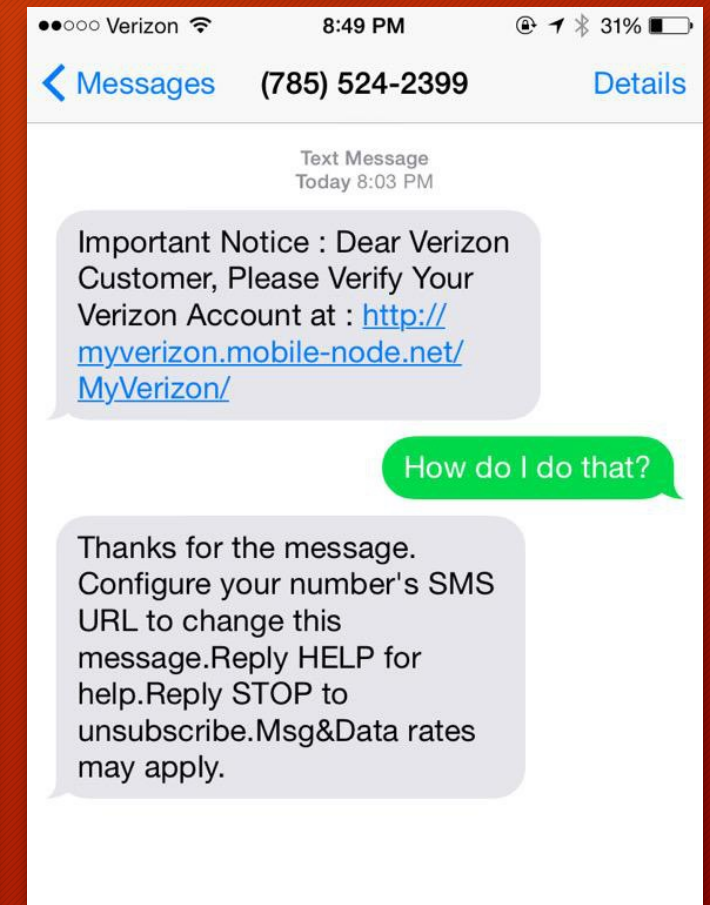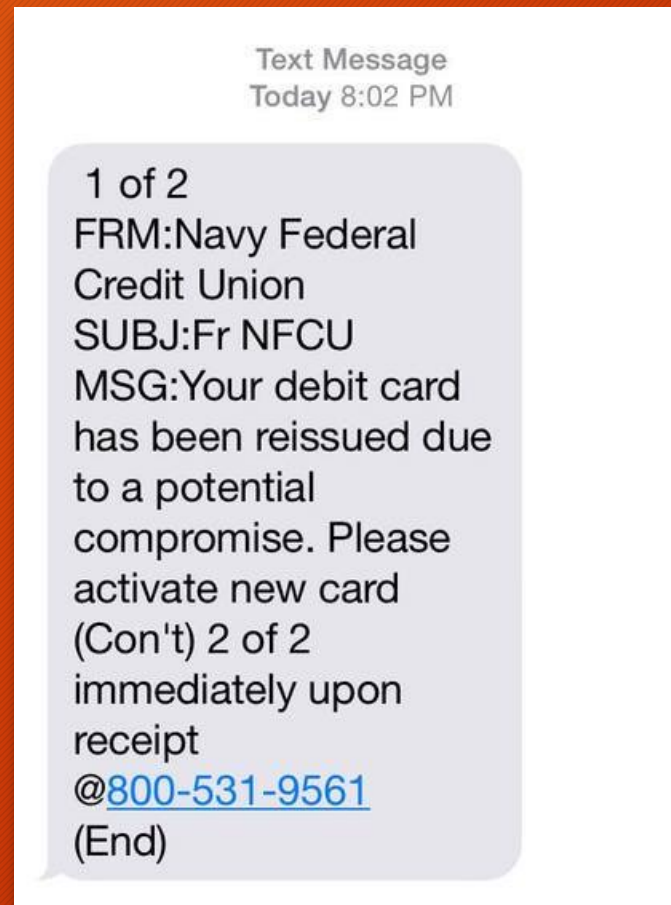
Looking Forward

- Adding more online resources for students to access 24/7 to help with remote and traditional learning

- Reducing the instructor to student ratios in lab courses to increase retention and allow for more timely assistance (Need not implemented)

- Because of the mistakes made during the extended virtual learning, we have a better understanding of what needs to be done to improve and offer more virtual learning opportunities for motivated students

Current Threats

How to minimize risk...

SMISHING

- SMS (text messages) are the fastest growing areas of social engineering

Text Message
Today 8:02 PM

1 of 2
FRM:Navy Federal
Credit Union
SUBJ:Fr NFCU
MSG:Your debit card
has been reissued due
to a potential
compromise. Please
activate new card
(Con't) 2 of 2
immediately upon
receipt
@800-531-9561
(End)

●●○○○ Verizon 📶   8:49 PM   @ ✈ ✳ 31% 🔋

‹ Messages   (785) 524-2399   Details

Text Message
Today 8:03 PM

Important Notice : Dear Verizon
Customer, Please Verify Your
Verizon Account at : http://
myverizon.mobile-node.net/
MyVerizon/

How do I do that?

Thanks for the message.
Configure your number's SMS
URL to change this
message.Reply HELP for
help.Reply STOP to
unsubscribe.Msg&Data rates
may apply.

Personal Mitigation

- Android and iPhone have password managers built into them
- Use recommended passwords from Apple/Google password suggestions – Automatically saves to device/account
- Have different passwords for EVERY account
- Protect your email account
- Have different email accounts for different purposes
  - Bills
  - News/Newsletters
  - Personal correspondence
  - Social Media
  - Online Shopping

Personal Mitigation Cont.

- Enable 2 factor authentication for all accounts (If they offer it)
  - Authentication apps like Google or Microsoft are best security
- Which authentication should I choose?
  - Authentication app is best security
  - SMS, Email, or Phone calls are only recommended if it is the ONLY option.
- What password managers can I trust?
  - https://bit.ly/3vb11JK

Personal Mitigation Cont.

- Turn off WiFi and Bluetooth when not using on phones
- Use a VPN for all internet traffic (especially when traveling)
- Limit account and personal exposure by deleting cookies when browser sessions close
- Use Private browsing when surfing the net
- Be skeptical of things and take time to see if there are any red flags that pop up before you click or answer
- DON'T FALL FOR "MILITARY GRADE…" It is a dumb marketing thing!

Questions?