

Why Multi-Factor Authentication (MFA)?

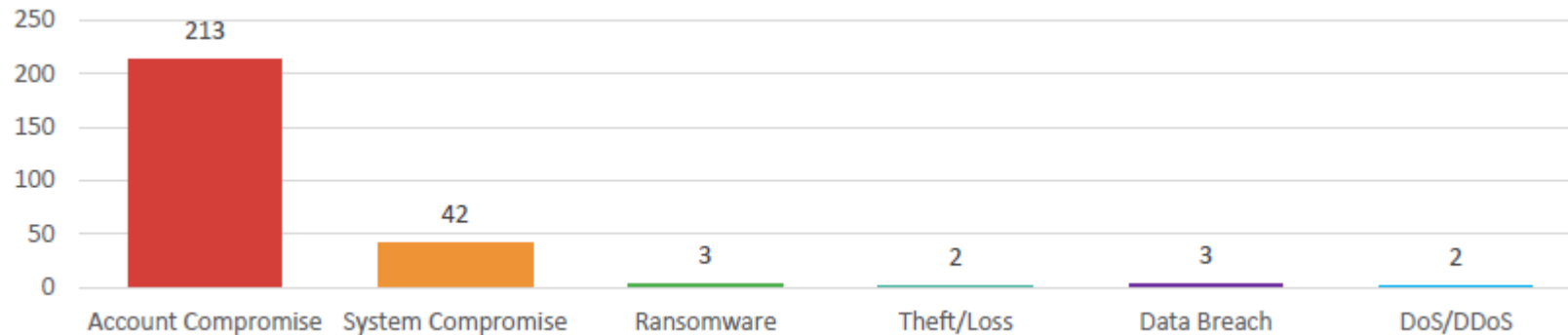
Chris Vakhordjian, Chief Information Security Officer
Ayesha Benjamin, Information Security Business Analyst

Agenda

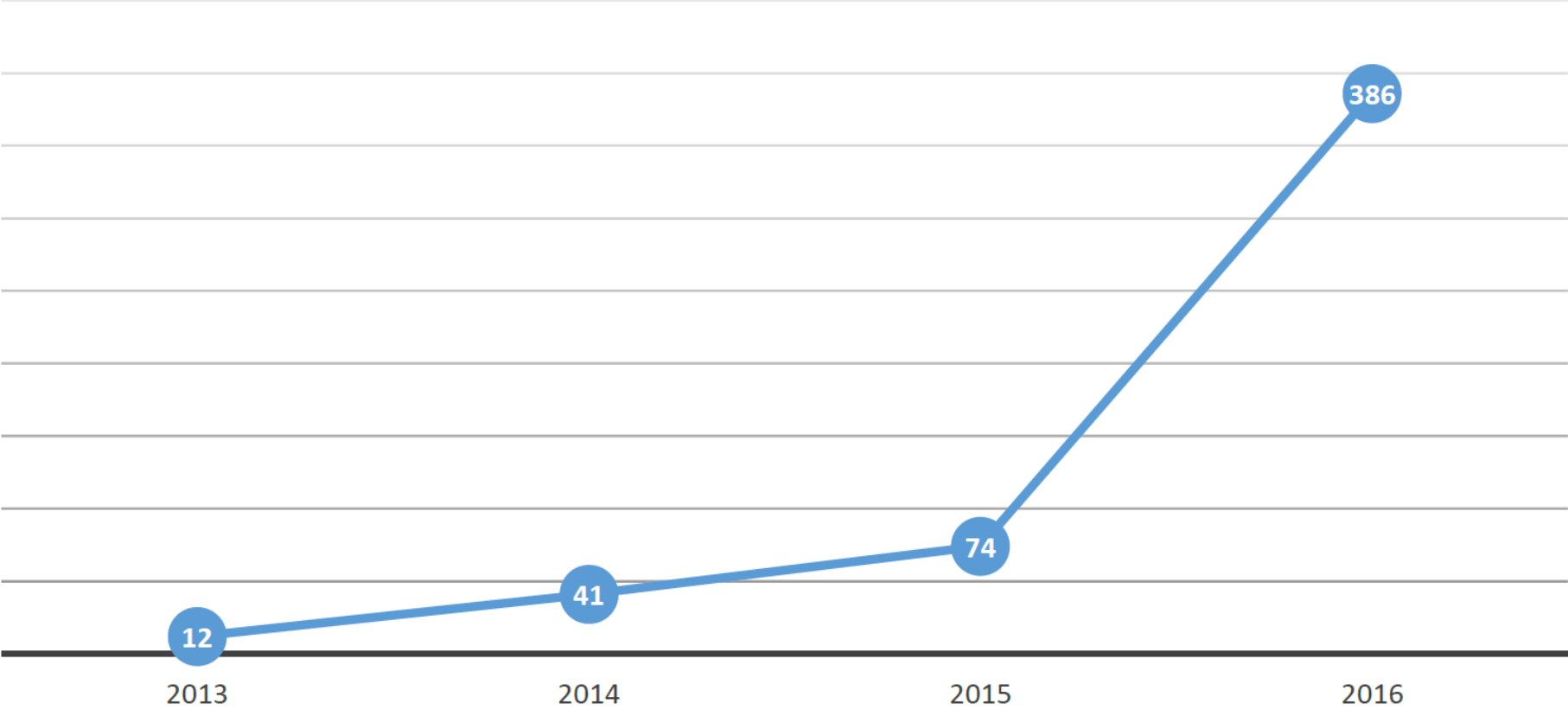
- 2016 Security Indicators
- Attack Vector
- The Problem
- The Solution
- DEMO
- Q&A

UCF is constantly under cyber attack

- Security Incidents in 2016



Phishing Campaigns Per Year?



How Many Phishing Incidents Occur Each Year?

Phishing

Phishing is the act of convincing someone to surrender their personal information (e.g., computer account and password, bank account information, social security number, etc.) that can then be used for identity theft, steal personal information, or commit other crimes.

- An example for this is a spoofed email purporting to be from an “official UCF office” or from a compromised UCF official/employee/etc. asking for your username and password, or providing a malicious link in an email for the user to login to a bogus website.

Example 1




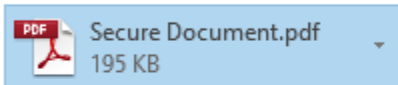
Mon 1/9/2017 10:01 AM

John C. Hitt <prescomments@mail.ucf.edu> <phargreaves@natomasunified.org>

Important Announcement from President John C. Hitt

To

 If there are problems with how this message is displayed, click here to view it in a web browser.



Dear UCF Family,

Please read attached for an important announcement from President John C. Hitt

Office of the President
University of Central Florida
P.O. Box 160002
Orlando, FL 32816-0002

Phone: 407-823-1823
FAX: 407-823-2264
Email: [Office of the President](#)

Example 2

 Fri 1/13/2017 9:21 AM
MyUCF <chippers@bell.net>
Directory
To

You have (2) important unread mails from the school Administrator,Kindly click on [review](#) to read it.

Consequences of Phishing

- Phishing campaign at UCF have successfully obtained our employees usernames and passwords and have targeted our employees direct deposit information.
- Attempts have been made to change direct deposit information on our faculty and staff to transfer paychecks to unauthorized banks.

The problem

- Authenticating to systems and applications with just username and password is insufficient.
- Potential for our employees using their UCF password on non-UCF systems or websites.
 - This means that an adversary who steals the password from some not-very-important website can look for @ucf.edu accounts, and try to log into UCF websites (e.g., myUCF portal) using the same password.
- Potential for weak passwords.

How MFA helps

- MFA is a mechanism used to protect systems, services, and accounts for which a password alone provides insufficient security.
- It is based on the principle of something you know (your username and password) and something you have (your smartphone, landline, time sensitive code, etc.)
- Users are first prompted to authenticate with their username and password; they are then prompted for a second authentication step using their phone, landline, or a time sensitive code.

Introducing MFA - DUO



- Early 2017 UCF purchased DUO for our MFA solution.
 - DUO licenses only cover employees (faculty/staff, not students at this time)
- Beginning April 19, UCF faculty and staff will need a second authentication factor for accessing certain sensitive pages in myUCF.
 - Retrieving W-2
 - Viewing and updating direct deposit information

DUO DEMO



How It Works



1. Enter username and password as usual
2. Use your phone to verify your identity
3. Securely logged in

Some Phases of MFA

- Protect myUCF W-2 & Direct Deposit information – April 19
- Protect myUCF for privileged users – Fall 2017
- Protect critical HR/Student/Financial and supporting systems and applications for privileged users – 2017/2018

Q&A

Thank you!