CYBER FRAUD

Presented by:

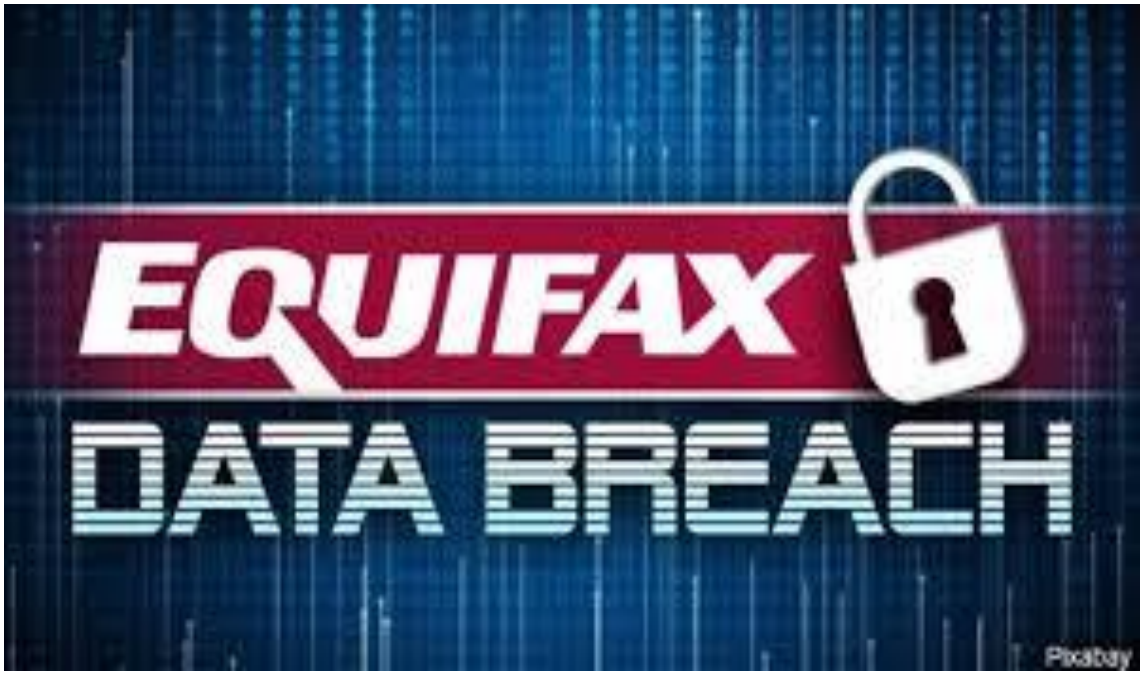
JACK R. SUDOL, MBA

stewart title®

Real partners. Real possibilities.™

stewart title
Real partners. Real possibilities.™

Cyber Fraud



stewart title
Real partners. Real possibilities.™

FBI Announcement

- Between October 2013 and December 2016 the FBI reported 40,203 incidents of BEC/EAC totaling **$5.3 Billion Dollars of Losses!**
- The number of wire fraud scams reported by title companies spiked 480% in 2016 *(ALTA article dated 5/9/17)*

stewart title
Real partners. Real possibilities.™

New Jersey Statistics

- 2016 Cyber Crime losses in New Jersey totalled $24,500,833.
- Of the top-30 Cyber Crimes we have:
  - 16.) Phishing
    - 575 Victims
    - $401,737 in Loss
  - 9.) Real Estate or Rental
    - 270 Victims
    - $1.35 Million in Loss
  - 1.) Compromised Email Accounts
    - 292 Victims
    - $8.69 Million in Loss

stewart title
Real partners. Real possibilities.™

Two Most Common Scams

- Business Email Compromise (BEC)
  - This scam targets those businesses that work with vendors and/or other businesses that perform wire payments.
- Email Account Compromise (EAC)
  - This scam targets individuals directly that perform wire transfer payments.

stewart title
Real partners. Real possibilities.™

Why are we here?

- Malware
- Spyware
- Ransomware
- *** Social Engineering
- *** Phishing

stewart title
Real partners. Real possibilities.™

Social Engineering

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme.

stewart title
Real partners. Real possibilities.™

Social Engineering Can…

- Learn about you (via LinkedIn, Facebook, etc.)
- Send infected attachments
- Install malware
- Deliver malicious links

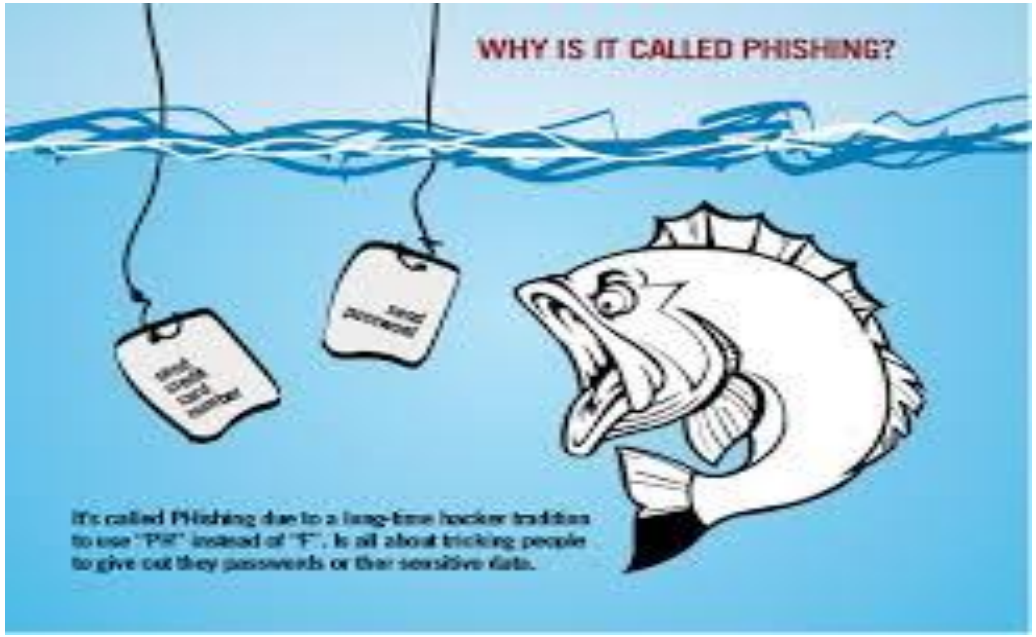
stewart title
Real partners. Real possibilities.™

Social Engineering Do's and Don't

- Keep your business and personal life separate
- Be suspicious of any URL links in emails
- Be aware of all email attachments
- Use reputable email services
- Protect your credentials
- Don't accept invitations from people you don't know

stewart title
Real partners. Real possibilities.™

Phishing



stewart title
Real partners. Real possibilities.™

Phishing

Is the attempt to obtain sensitive information for malicious reasons and monetary gain by disguising a trustworthy entity in an electronic communicator. Phishing schemes are usually addressed to the target and contain relevant content as a result of thorough research.

stewart title
Real partners. Real possibilities.™

Phishing can lead to…

- Credential harvesting
- Redirecting to malicious websites
- Installing malicious software
- Downloading malicious attachments

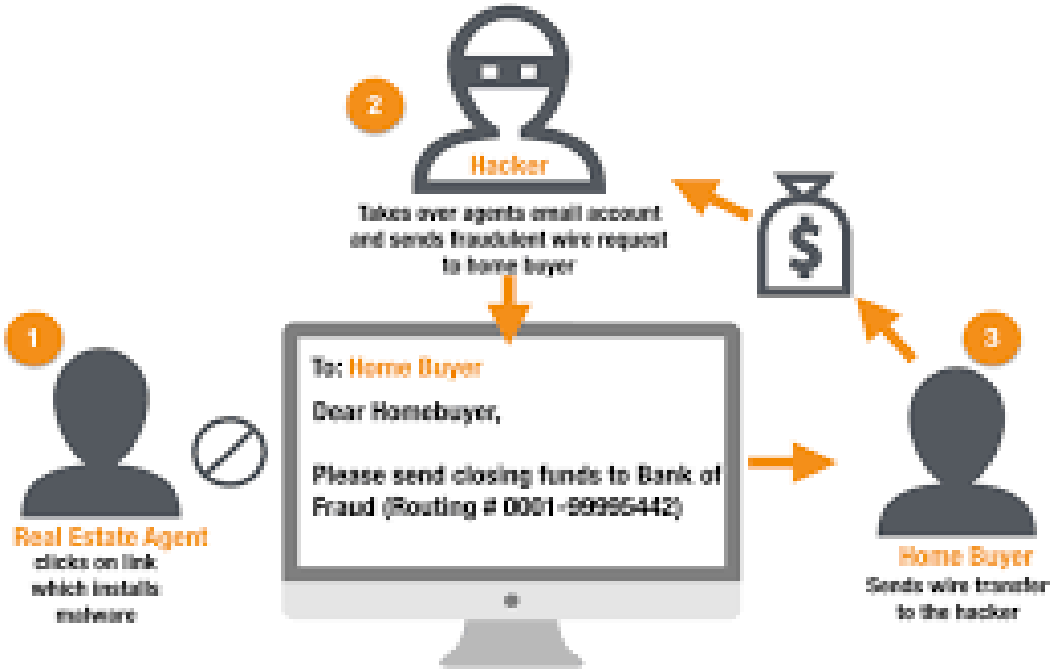
stewart title
Real partners. Real possibilities.™

Phishing Do's and Don't

- Scrutinize every link
- Go to websites directly
- Beware of attachments
- Keep your operating system and browser up to date
- Don't download attachments you are not expecting
- Don't click on links
- Don't respond to original emails

stewart title
Real partners. Real possibilities.™

Anatomy of a Wire Fraud



stewart title
Real partners. Real possibilities.™

Watch for Red Flags

- Misspelled email domains
  - Double letters
  - Look-a-likes
  - Vowels replaced
- Different email domains
  - Free domains
- Changes in the footer
- Changes in the style

stewart title
Real partners. Real possibilities.™

For individuals

- Don’t click on links embedded in emails
- Download software only from trusted sources
- Unplug your internet connection when you’re away
- Don’t send sensitive files over Wi-Fi or “hot spots”
- Never reply to emails that ask for personal information

stewart title
Real partners. Real possibilities.™

For Companies

- Avoid free web based emails – use private domain email address
- Encrypt your email communication that contains NPI
- Limit or ban access to social media websites on office computers
- Include a warning in your email signature
- Confirm wiring instructions before sending emails

stewart title
Real partners. Real possibilities.™

For Companies

- Use the “Forward” option rather than the “Reply” option to respond to business emails
- Fax wiring instructions
- Consider implementing a “two-factor” authentication to confirm requests for transfer of funds
- Scrutinize all email requests for transfer of funds and beware of sudden changes in business practices.
- Obtain Cybercrime coverage

stewart title
Real partners. Real possibilities.™

Best Practices

- Obtain an Escrow Security Bond with Cyber Coverage to protect against fiduciary losses
- Reconcile escrow/trust accounts timely
- Adhere to ALTA best practices

stewart title
Real partners. Real possibilities.™

Thank You

Questions?