CYBERSECURITY AWARENESS EXERCISE FOR JUDGES RECAP

Stewart R. Bruner
TAC
August7, 2015

DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack cyber criminals use to trick or fool you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or well known store. These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or falling for a scam.

Cyber criminals craft these convincing looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know the more emails they send out, the more people they will hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging and SMS.

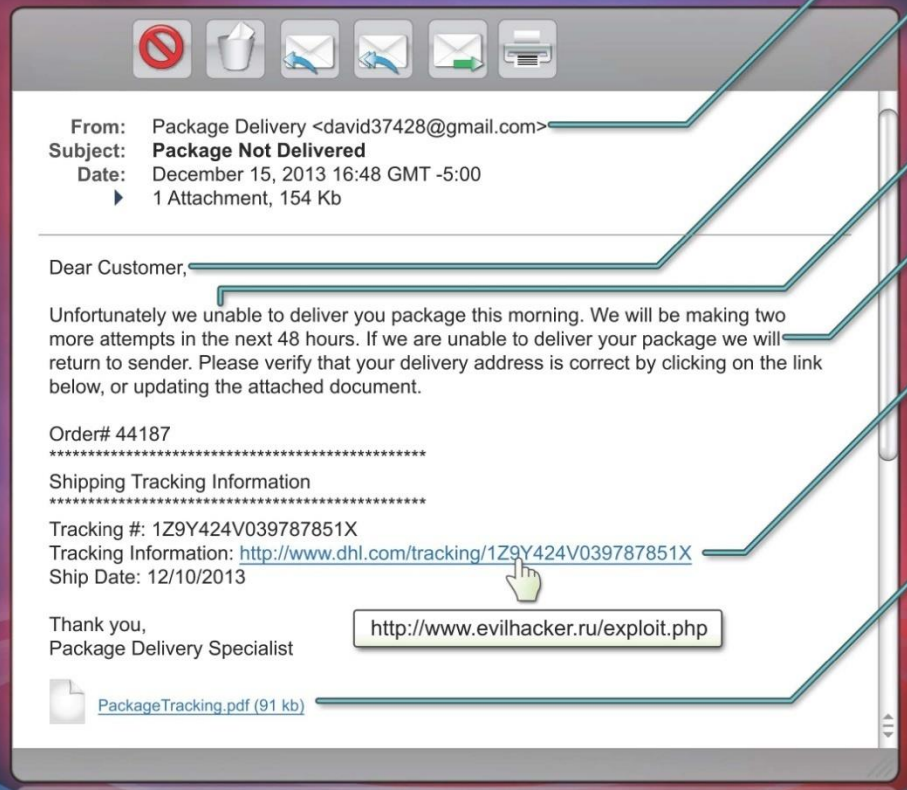
WHAT IS SPEAR PHISHING?

The concept is the same, however instead of sending random emails to millions of potential victims, cyber attackers send spear phishing messages to a very few select individuals, perhaps five or ten targeted people.

With spear phishing the cyber attackers research their intended targets, such as reading the intended victim's LinkedIn or Facebook accounts or any messages they posted to public blogs or forums. Based on this research, the attackers then create a highly customized email that appear relevant to the intended targets. This way, the individuals are far more likely to fall victim to the attack.

WHY SHOULD I CARE?

You may not realize it, but you are target, not only at work but at home. You and your devices are worth a tremendous amount of money to cyber criminals and they will do anything they can to get it. The number one way cyber criminals are hacking people like you is with a technique called phishing. However you are also one of the most effective ways we can detect and stop a phishing attack. If you identify an email you feel is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing visit www.securingthehuman.org/phishing.



INDICATORS OF A PHISH

A Check the from email address. If the email appears to come from a legitimate organization, but the From address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack .

B Be suspicious of emails addressed to "Dear Customer" or some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information.

C Be suspicious of grammar or spelling mistakes, most businesses proofread their messages carefully before sending them.

D Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake.

E Be careful with links, only click on links that you were expecting. Also, hover your mouse over the link. This shows you the the true destination of where you would go if you click on it. If the true destination is different then what is shown in the email, this is an indication of an attack.

F Be suspicious of attachments, only open attachments that you were expecting.

G Be suspicious of any message that sounds too good to be true (no you did not win the lottery).

H Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, use a reliable phone number for verification.

GOAL: REINFORCE SPEAR PHISHING AWARENESS FOR JUDGES

COJET requirement changed for 2015 – now mandatory cybersecurity

Decided on SANS one-page handout for conference attendees

Got lunchtime speaking slot for Thursday, June 18

Reviewed lessons learned with Phoenix from 2013 phishing exercise

Targeted 510 registered judges with Ed Services help

- No state bar or law firm addresses used, but court & personal addresses OK

Created Wordpress site, gmail account, voicemail box

Tested to ensure deliverable, reachable thru firewall

Obtained management approval, set counter on website

Sent e-mail Thursday, June 11 @ 2PM

Checked hits on website Monday June 15 @ 9AM

HERE IS THE BAIT

Reply Reply All Forward IM

Wed 6/10/2015 1:29 PM

Arizona Education Services Division <azedu

IMMEDIATE ACTION NEEDED: AZ Judicial Conference Re-Registration

To

Dear Hon. Judge, Commissioner, or Pro Tem;

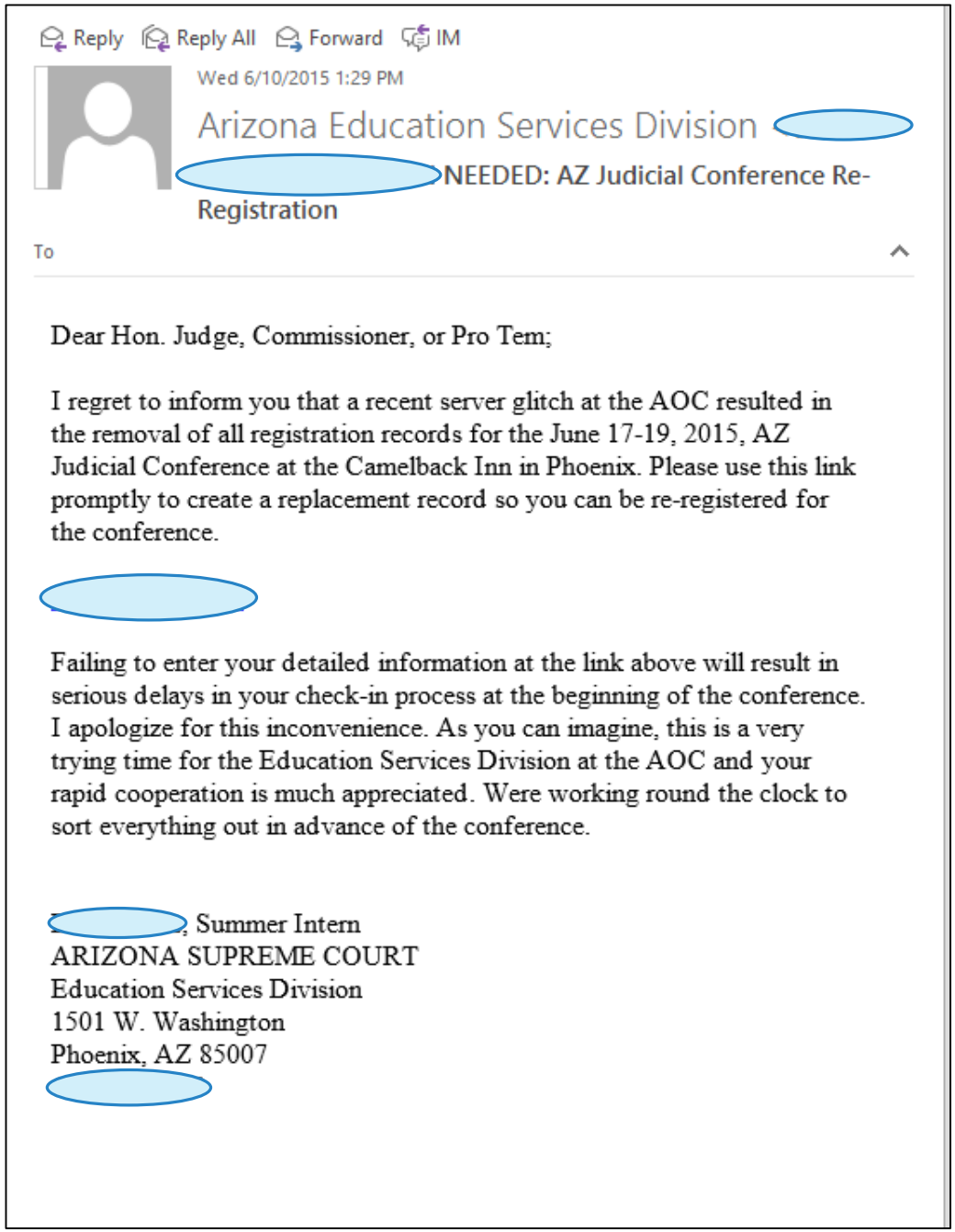
I regret to inform you that a recent server glitch at the AOC resulted in the removal of all registration records for the June 17-19, 2015, AZ Judicial Conference at the Camelback Inn in Phoenix. Please use this link promptly to create a replacement record so you can be re-registered for the conference.

Registration Link

Failing to enter your detailed information at the link above will result in serious delays in your check-in process at the beginning of the conference. I apologize for this inconvenience. As you can imagine, this is a very trying time for the Education Services Division at the AOC and your rapid cooperation is much appreciated. Were working round the clock to sort everything out in advance of the conference.

Evan White, Summer Intern
ARIZONA SUPREME COURT
Education Services Division
1501 W. Washington
Phoenix, AZ 85007
602-452-3998

WARNING SIGNS



Reply Reply All Forward IM

Wed 6/10/2015 1:29 PM

Arizona Education Services Division

NEEDED: AZ Judicial Conference Re-Registration

To

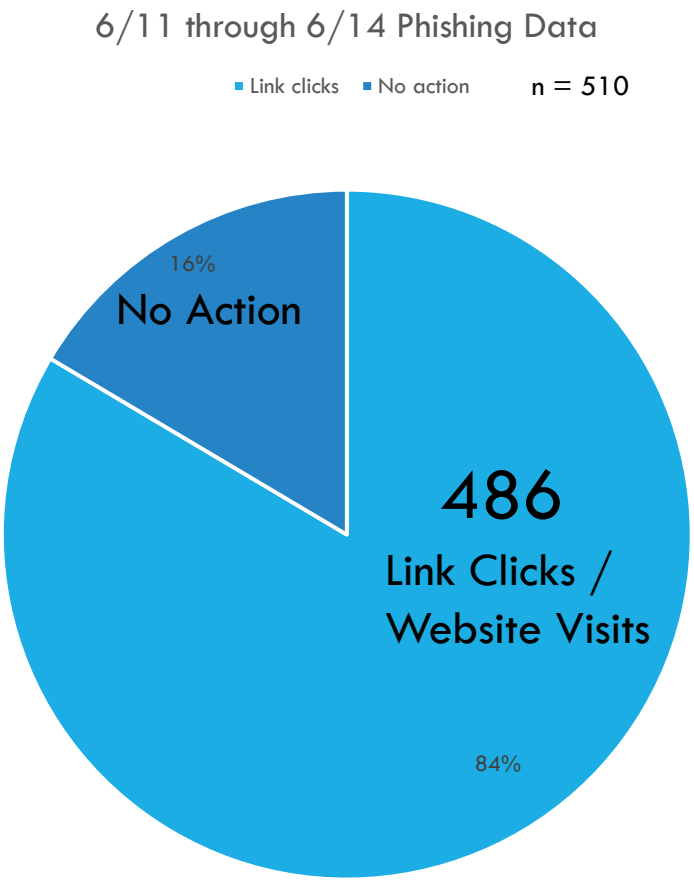
Dear Hon. Judge, Commissioner, or Pro Tem;

I regret to inform you that a recent server glitch at the AOC resulted in the removal of all registration records for the June 17-19, 2015, AZ Judicial Conference at the Camelback Inn in Phoenix. Please use this link promptly to create a replacement record so you can be re-registered for the conference.

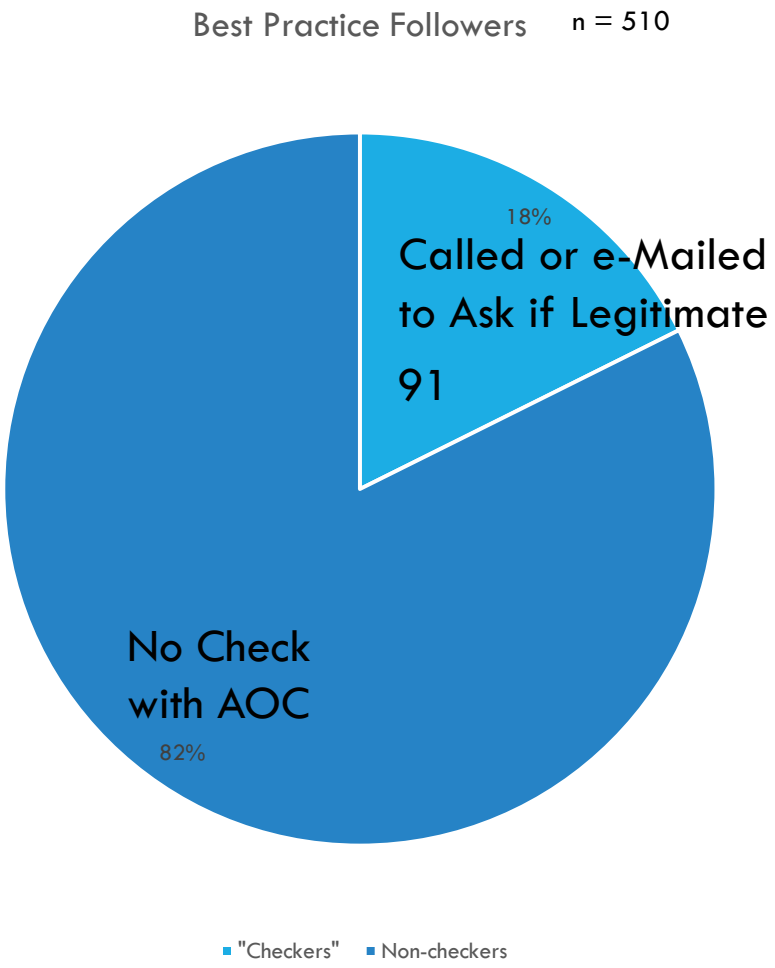
Failing to enter your detailed information at the link above will result in serious delays in your check-in process at the beginning of the conference. I apologize for this inconvenience. As you can imagine, this is a very trying time for the Education Services Division at the AOC and your rapid cooperation is much appreciated. Were working round the clock to sort everything out in advance of the conference.

, Summer Intern
ARIZONA SUPREME COURT
Education Services Division
1501 W. Washington
Phoenix, AZ 85007

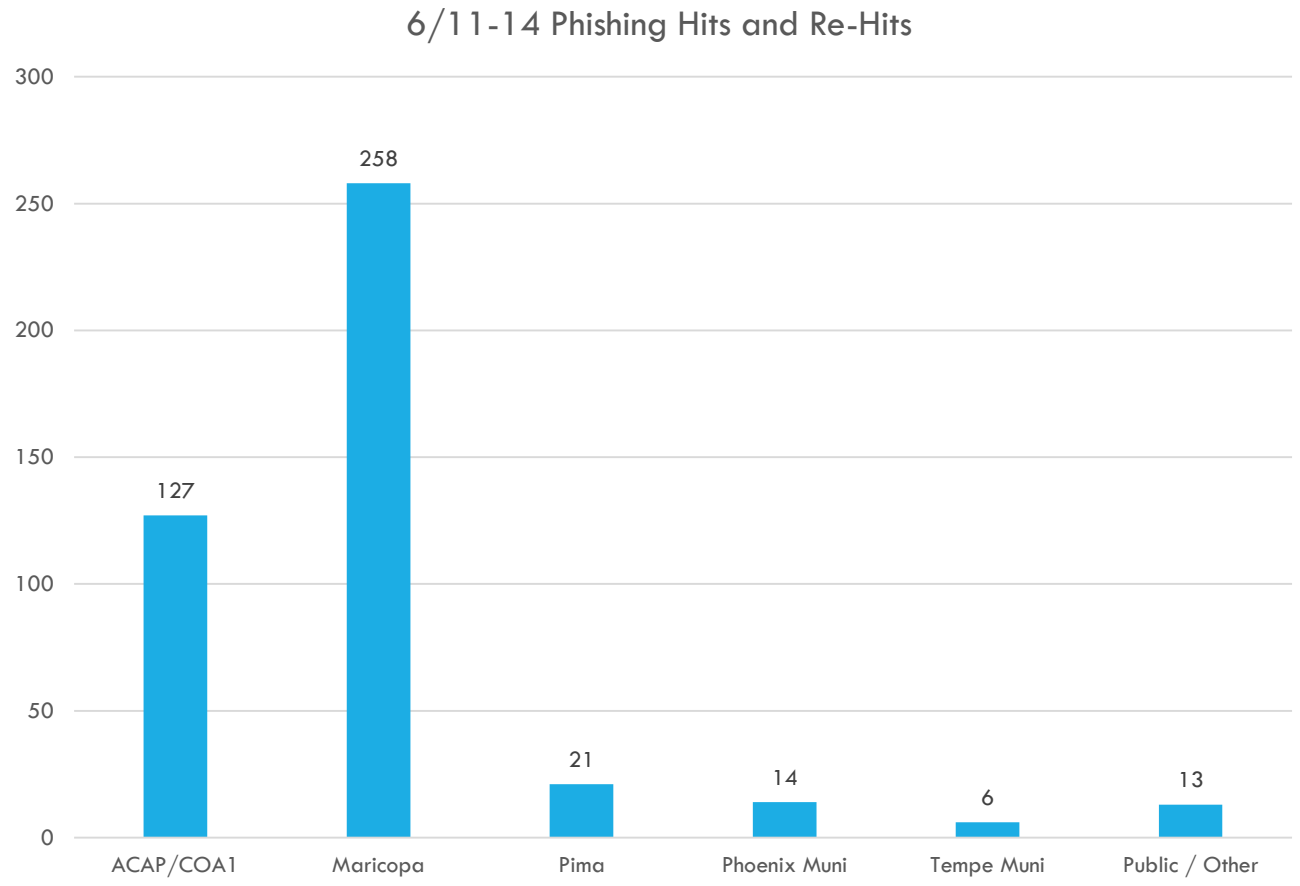
WHAT THE DATA SHOWS



TO BE FAIR…


Best Practice Followers
n = 510
18%
Called or e-Mailed to Ask if Legitimate
91
No Check with AOC
82%
"Checkers"
Non-checkers

WHERE CLICKS ORIGINATED, MOST LIKELY



WHAT COULD THAT LINK DO?

1. Install malicious code on your computer, like ransomware, without your awareness.
2. Send bogus e-mails appearing to be from you to everyone in your contacts/address book, perpetuating the phishing scheme.
3. Start a key logger and communication redirect in the background to ship your IDs and passwords to a server overseas.
4. Add your machine as a botnet client to be used in future denial of service attacks against websites.
5. Send you to a “look-alike” website of a company or government entity you trust to extract IDs, passwords, or personal information from you.