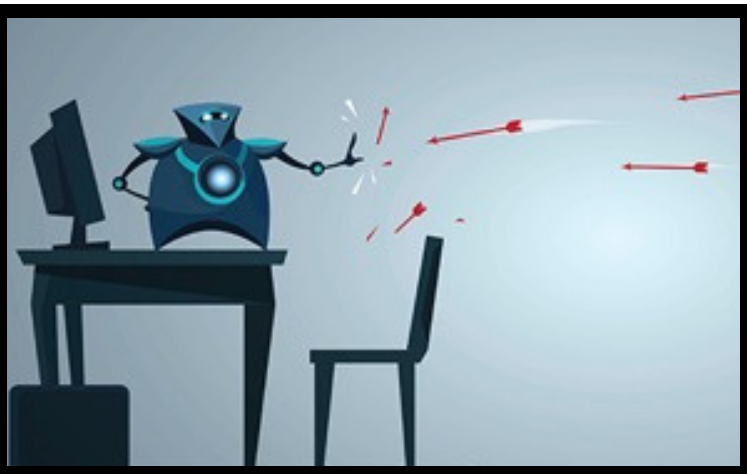
CS Bits and Bytes
Highlighting Innovative Computer Science Research
Vol 5, Issue 9

DETECTING PHISHING

Phishing attacks are used to trick online users to provide sensitive information, such as passwords or credit card numbers. Even though cybersecurity measures exist to stop phishing, attackers constantly change their tactics to deceive users and evade detection. Research combining human and computer intelligence is helping to combat this problem.



HOW DOES IT WORK?

Phishing attacks that are constantly changing are difficult to detect because they cannot easily be defined or classified. To solve this problem, computer systems are trained to identify the key characteristics of attacks by sending both true and false instances of phishing. The systems build a set of rules for what a phishing attack looks like, and these rules, or the algorithm, learn to better classify and identify attacks.

PHISHERS, BEWARE

If a message doesn't follow the rules of the algorithm, computer systems cannot confidently classify it as a legitimate or fake attack. By sending the message to experts who use their own knowledge to identify traits of the message that the computers couldn't recognize, the algorithm is adjusted. This improves the systems' ability to recognize attacks. This combination of machine learning and crowdsourcing is helping researchers build more accurate and reliable defense systems against phishing.

THE BOTTOM LINE ▶ People work with computers to catch a phish!

GANG WANG

Basketball, video games, playing Legos with his kids

> ***Don't be afraid to break things!***
>
> ... as long as it is legal and ethical. You can learn a lot by tearing a computer system apart. Start with something simple such as a programmable toy or a smart phone app.

THE SECURITY EXPERT

Gang Wang is an assistant professor of computer science at Virginia Tech. His research focuses on developing methods to thwart increasingly disruptive and dangerous cybersecurity threats. His work has earned him several awards; he is the recipient of a NSF CAREER Award and a Google Faculty Research Award.

LEARN MORE:

Psst...This Bits & Bytes feature contains hidden links! When the mouse changes from an arrow to a hand icon, click on the content to learn more.

CS Bits and Bytes

Highlighting **Innovative** Computer Science Research

TYPES OF PHISHING

Phishing

Attempting to decieve an online user to provide confidential information by disguising as a tustworthy entity

Spear phishing

Phishing attempt that targets a specific person or entity, where the attacker users information about their target to increase the probability of success

Domain squatting

Impersonating legitimate web pages often by registering domain names that mimic the real ones; also called cybersqatting

WHAT DO YOU THINK?

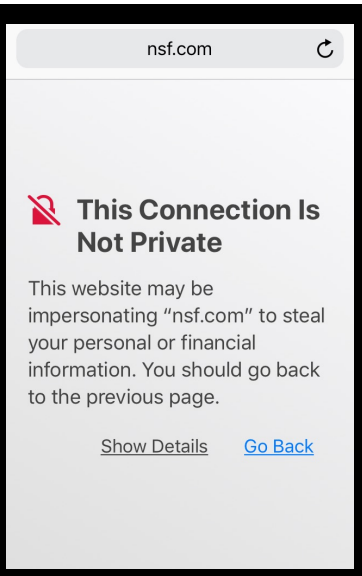
Can you outsmart internet scammers? Take **this quiz** and see if you recognize the different types of phishing attacks!

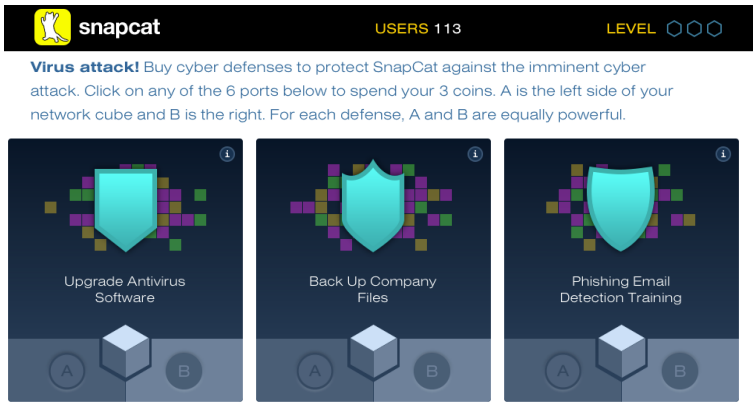
PHISH REAL

DOMA1N SQUATT1NG

Social media platforms are particularly at risk for cyber attacks that involve phishing because of the data they collect from users.

With domain squatting, attackers will use a domain name, or the website's IP address, to mimic the real site. For example, attackers may have registered domain names with common misspellings that a user might not notice when trying to quickly navigate to a site. Some attackers even use international characters to fool people.





TRY IT OUT!

Learn what it's like to be the head of a start-up social network company under increasingly sophisticated cyber attacks. In the **NOVA Cybersecurity Lab** you will work with a technologically-savvy entrepreneur to grow your tiny company into a global empire!

Links in this issue:
https://bit.ly/2u7c08j
https://bit.ly/2IquBWq
https://bit.ly/2FbgSQg
https://bit.ly/2W13p2O
https://bit.ly/2VZmxyg
https://to.pbs.org/2CjHQn4

Photo credits:
JobsCorp.gov
Mai Khanh Nguyen
The VERGE

Created by Allyson Kennedy and Sharon McPherson