fhwedel
UNIVERSITY OF APPLIED SCIENCES

Bleeding Edge Technology

By: Husnain Khan

Supervisor: Prof Dr. Gerd Beuster

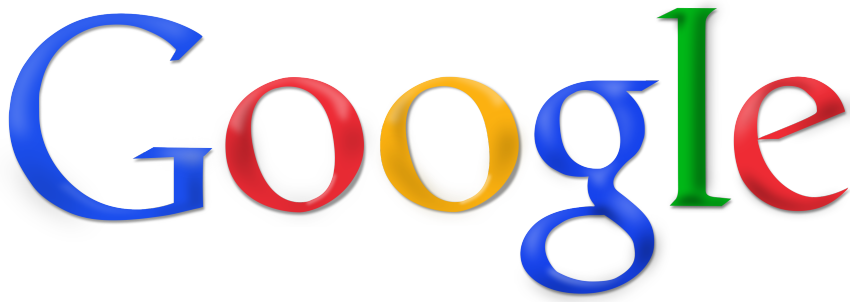
Date: December 2, 2021

What is Bleeding Edge Technology?

- **technology released in the market without undergoing extensive testing**
- **can pose a certain amount of threat to consumer's privacy and security as they are usually target of hacking and security breaches**

How is that different from ”Leading Edge/ Cutting Edge”?

- **“cutting/ leading edge technology” refers to software that has been well-established in the market and is a step ahead of its competitors therefore is more reliable and poses less threat to consumer’s security.**



Then why use Bleeding Edge Technology?

- **Cost efficient**
- **Allows time to fix glitches in original software**
- **Users can provide feedback that can be used to modify technology to cater their needs**
- **Has potential to becoming Leading Edge.**

What applications are most targeted for security breaches?

1. **Online Computer Games**

2. **Web Applications**
   - eBay
   - Social Networking Sites (Facebook, Instagram, Twitter)

3. **Electronic Elections**

4. **Cryptocurrencies.**

Online Computer Games

- **GDP of Online computer games larger than some small countries!**

- **In 2001, game sales hit $9.4 billion in USA surpassing movie-box office sales**

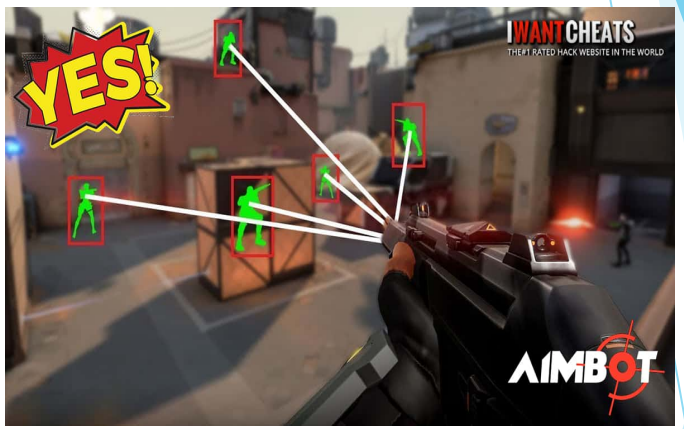
- **<u>How does cheating in games hurt game developers?</u>**
  - Cheaters can gain unfair advantage via hacking and security breaches which can lead to biases in the game and over-time consumers loose interest dropping overall demand of the game.

Types of Cheating in Online Computer Games

Type	*Label*	*Cheating Form*
Of special relevance to online games	A	Cheating by Exploiting Misplaced Trust
	B	Cheating by Collusion
	C	Cheating by Abusing the Game Procedure
	D	Cheating Related to Virtual Assets
	E	Cheating by Exploiting Machine Intelligence
	F	Cheating by Modifying Client Infrastructure
	H	Timing Cheating
Generic	G	Cheating by Denying Service to Peer Players
	I	Cheating by Compromising Passwords
	J	Cheating by Exploiting Lack of Secrecy
	K	Cheating by Exploiting Lack of Authentication
	L	Cheating by Exploiting a Bug or Design Loophole
	M	Cheating by Compromising Game Servers
	N	Cheating Related to Internal Misuse
	O	Cheating by Social Engineering

Aimbots

- Aimbots are cheating mechanism where a cheater can enhance their aim compared to normal human or completely have a bot perform all of the target shooting.



- Used in First Person shoot games to aim at better target

- Can also be used in virtual economical games to do tedious tasks such as collecting coins and objects.

- done by tampering with the code and making up own version of the code which can provide automation and support

How are Aimbots Detected?

1. **Authentication and Encryption mechanisms**
2. **Game guard such as Punkbuster**
3. **“AimDetect”**
   - relies on Performance-Skillfulness inconsistency in the player to detect cheating.
   - Cheater better at aiming/ shooting but lacks skills such as defending and situation awareness

- **<u>Ways to escape AimDetect?</u>**
  - via mimicking a normal user behaviour in which initially the cheater performs as an average player and gradually increases performance to mimic improvement and becoming more skillful via practice

Security Breaches in Web Applications

- **Web Applications include sites such as Google, eBay, and Hotmail**
- **Security breaches occur via:**
  - SQL injections
  - Cross- site scripting (XSS)

- **These breaches have potential to steal, edit and destroy database of web-applications.**

eBay

- auction site used world-wide to buy and sell different goods and is linked to PayPal, a payment service company
- Target for old-fashion frauds such as scamming and also phishing
- Often target of Phishing attacks because linked to payment/ banking information

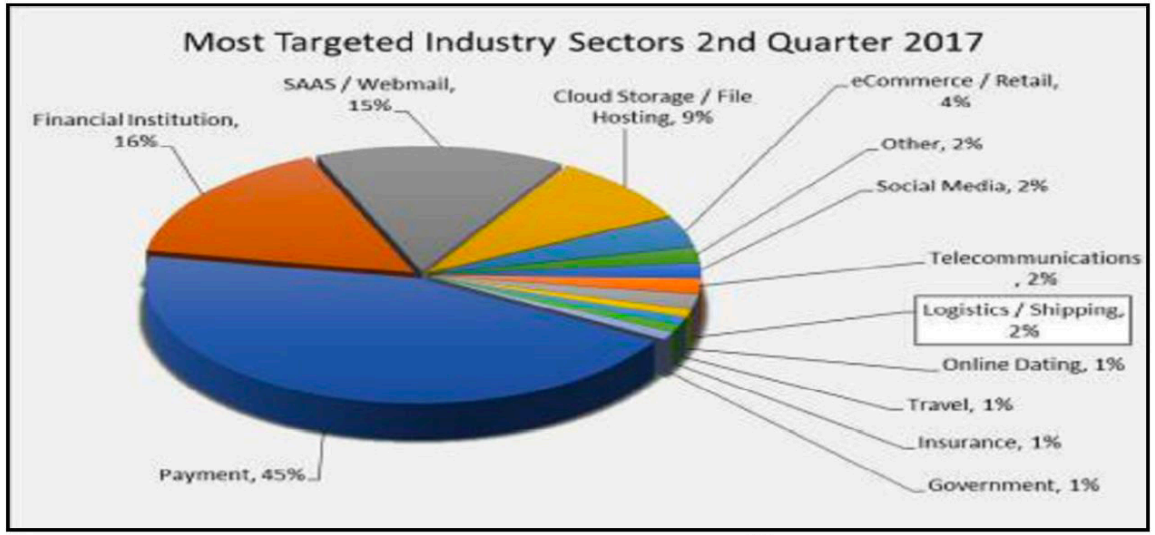


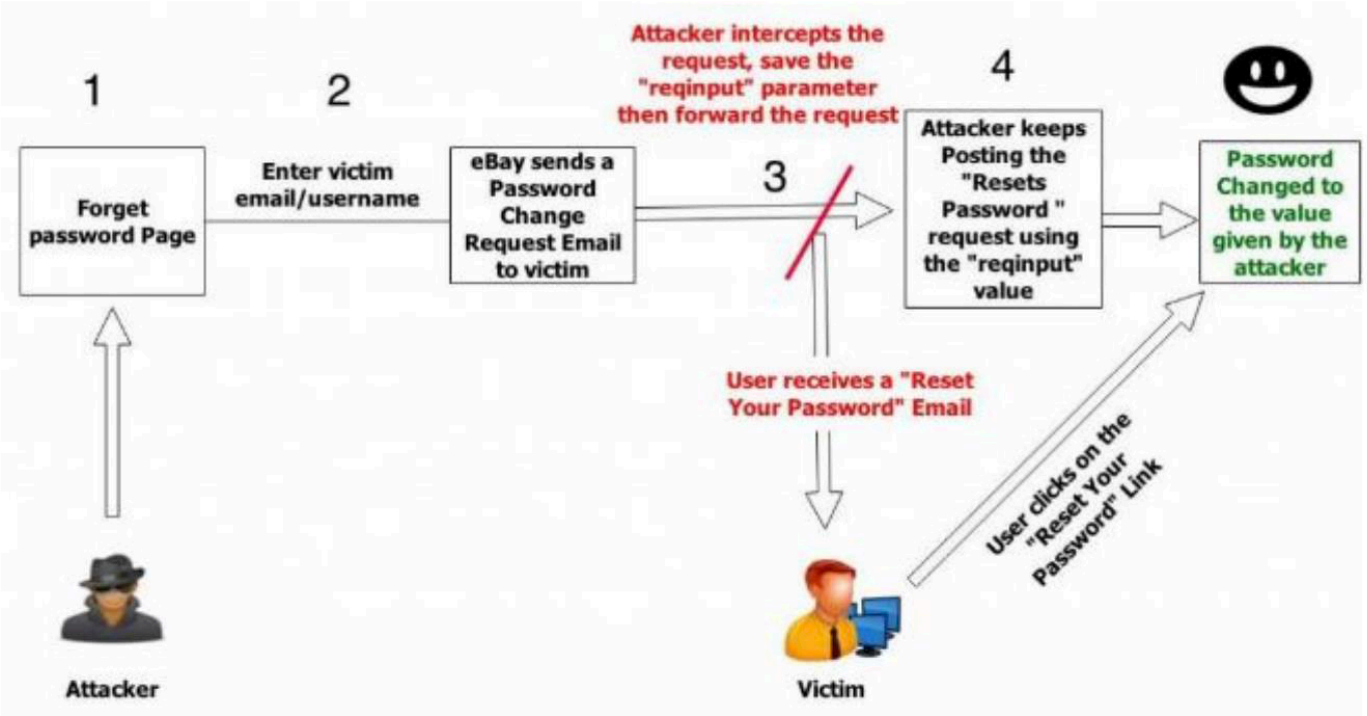
Fig 1: Most targeted industry sectors 2nd quarter 2017

How does Phishing work?

- **cyber-attack in which user is tricked into clicking on a link, e-mail or open a website which leads to installation of malicious malware in their machine, hijacking the machine and revealing sensitive information such as banking and other credentials to the hacker**

Example of Phishing

- **Phishing scam that utilizes a bug in “Forgot Password” process.**



Social Networking Sites

- include many different platforms such as Facebook, Instagram
- Security breaches can be very damaging not only because private information is leaked, but can also be accessed by employers and negatively impact a person.
- Platform where a lot of bullying occurs specially in Teenagers increasing suicide rates.

“Tagging” on Facebook

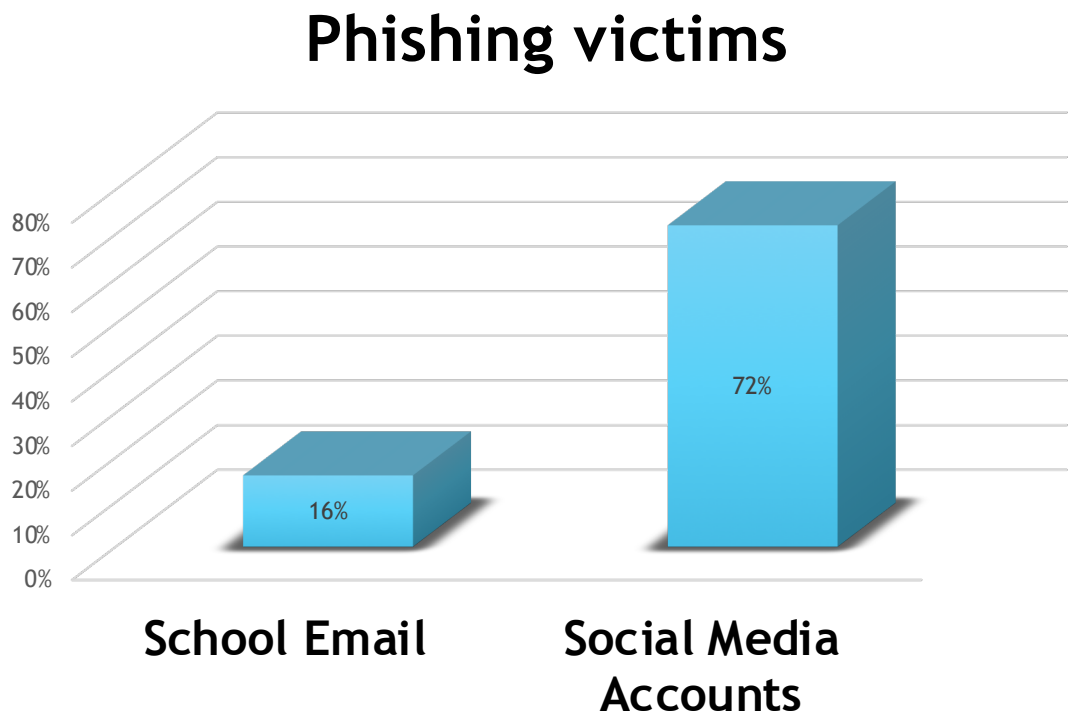
- **Can lead to private information being jeopardized even if you did not post that information, but a friend did and you failed to “opt out” of the tag.**

- **<u>Example:</u>**

“On New Year’s Day 2008, following the assassination of Benazir Bhutto in Pakistan, the UK press published a photo of her son and political heir Bilawal Bhutto, dressed up in a devil’s costume with red horns for a Halloween party, which was found on the Facebook site of one of his student friends”

Social Media accounts and hacking

- According to a study at Indiana University where an experiment was performed by sending phish to students on university email vs social network accounts. While 16% students became a target of phishing when email was sent to university email vs 72% individuals when sent to social network accounts



Security Measures used by different social networking applications.

TABLE I. COMPARATIVE ANALYSIS OF SOCIAL MEDIA SECURITY TOOLS

Security tools	Social media		
	Facebook	*YouTube*	*Instagram*
Two-factor authentication	+	+	+
Private account	+	+	+
Login notification	+	+	-
Security checkup	+	+	-
Trusted contacts	+	-	-
Identification code	+	+	+
Password strength checker	+	+	+
Password breaches checker	-	-	-
E-mail breaches checker	-	-	-
Periodic password changes	-	-	-
External application/site access checkup	+	+	-

Electronic Elections

- **Major concerns:**
  1. Satisfaction of voters that their vote will be counted
  2. Anonymity → to avoid vote-buying and Intimidation by the electoral candidates
  3. Computational Propaganda and Fake news media
  4. Cyberattacks
  5. Faulty equipment

Computational Propaganda and Fake News Media

- Fake news is propagated onto social media accounts to influence elections
- observed in many countries during election process such as Brazil, UK, France, USA, and Ukraine
- **via use of algorithms, automation, sockpuppet accounts and bots**
  - Bots used on Twitter to rebroadcast content
    - Dampener Bots → to supress messages
    - Amplifier Bots → to make messages appear much more popular than they really are
  - Sock puppets → human operated accounts that post fake news.

Cyberattacks to influence Elections

- Leaked Emails of Hilary Clinton during 2016 USA presidential Electoral Elections

- Data leak of emails and documents 2 days before election in 2017 French presidential elections campaign of Emmanuel Macron

Cryptocurrency

- **Hackers and Scammers sells cryptocurrencies on black market for Cash**

- **Easier to manipulate with cryptocurrencies because they are not yet regulated in most countries**

“Squid Game” Cryptocurrency scam

- **Scam of digital token inspired by popular south Korean Netflix series Squid Game, where buyers were scammed and lost $3.38 Million**

Bleeding edge technology comes with its cost, but has potential to become leading edge once major flaws are taken care off!

References

- *Bleeding Edge*. (n.d.). https://www.execuspeakdictionary.com/word-of-the-day/bleeding-edge-2/
- https://9gag.com/gag/a81WOnV
- https://coingenius.news/from-2-trillion-mcap-to-almost-zero-squid-coin-scammers-make-3-3-m-will-sec-intervene/
- https://www.greenandgrowing.org/hillary-clinton-stressed/
- https://www.tellerreport.com/news/2020-01-13---macron-stressed-the-importance-of-maintaining-a-ceasefire-in-the-donbass-.HJigK2Yg8.html
- http://www.riazhaq.com/2008/01/bilawal-bhutto-zardari-in-devil-costume.html

THANK YOU