WEEK 3 GLOSSARY AND REFERENCES

1

1-Click

1-Click, also called one-click or one-click buying, is the technique of allowing customers to make online purchases with a single click, with the payment information needed to complete the purchase having been entered by the user previously.[1] More particularly, it allows an online shopper using an internet marketplace to purchase an item without having to use shopping cart software. Instead of manually inputting billing and shipping information for a purchase, a user can use one-click buying to use a predefined address and credit card number to purchase one or more items. (via Wikipedia)

A

Ad blocker

Ad blockers are software programs and browser extensions that prevent unwanted advertisements, advertisement tracking, popups and malware while browsing.

Authentication

Authentication is the process of ensuring that the identity claimed by an entity is the correct one (see identification for further details). This is typically done by asking the entity to provide something they know, like a password, something they have, like a smart card, or something they are, like a fingerprint.

B

Boiler room fraud

Cold calling people to pressure them into buying shares that promise high returns. In reality, the shares are either worthless or non-existent. (via http://www.actionfraud.police.uk/fraud-az-boiler-room-fraud)

C

CVV

Card Verification Value is the 3 digit value on the back of many payment cards.

Cyber Monday

The Monday after the US Thanksgiving holiday has been named as “Cyber Monday”. It is primarily a marketing tool, encouraging online shopping and sales prior to Christmas.

D

Dark Web

The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but which require specific software, configurations or authorization to access.The dark web forms a small part of the deep web, the part of the web not indexed by search engines. (via Wikipedia)

DoS

A Denial of Service attack is where an attempt is made to make a computer or network resource unavailable to intended users. These are often targeted at high profile sites or services.

I

Identification

Identification is the process of associating an entity in the system, such as a resource or a user, to a proper identity, for instance an IP address or a name. Authorisation policies are usually defined based on the identity of the entities, rather than on the entities themselves, and two entities sharing the same identity will be indistinguishable.

Internet of Things

Everyday objects which have network connectivity. The Internet of Things Global Standards Initiative agreed on this definition: *a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.* In other words: The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

P

Phishing

Obtaining personal details (passwords, financial details) through trick emails and websites which appear to be from reputable sources.

R

Ransomware

A ransomware is a particular type of virus which, once installed on a computer, encrypts some particularly important files (e.g., Word or Powerpoint documents), and asks for a ransom to the owner, threatening to delete the encryption key unless the owner pays the ransom.

S

Secondary information

This is information that you have not shared directly. It's often related to your online activities such as browsing, purchasing, website visits and searches. It can be collected without you knowing, perhaps as a result of other people sharing information.

X

XACML

XACML stands for eXtensible Access Control Markup Language, a standard developed to define a declarative fine-grained, attribute-based access control policy language, an architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies.

References

The following references are linked from various articles in the course and brought together here, for further reading if you're interested in exploring the research in more detail.

Egelman, S., Herley, C. and Van Oorschot, P.C. (2013). Markets for zero-day exploits: Ethics and implications. In Proceedings of the 2013 workshop on New security paradigms, pp. 41-46. ACM.

Finifter, M., Akhawe, D. and Wagner, D. (2013). An empirical study of vulnerability rewards programs. Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13), pp 273-288.

Kahneman, D. (2013), *Thinking Fast and Slow*, Farrar, Straus and Giroux

Lampson, B., (1971), Protection. Proc. 5th Princeton Conf. on Information Sciences and Systems, Princeton, 1971. Reprinted in ACM Operating Systems Rev. Vol. 8, No 1, pp. 18-24.

Warren, S.D. and Brandeis, L.D. (1890). *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, pp. 193-220.

Westin, A.F. (1967). *Privacy and Freedom*, New York: Atheneum.