Cyber Security Awareness Training

Glossary

Bluesnarfing

The act of stealing personal data, specifically calendar and contact information, from a Bluetooth enabled device.

Botnet

A botnet is a network of infected computers that communicate with each other in order to perform the same malicious actions, like launching spam campaigns or distributed denial-of-service attacks. The network can be controlled remotely by online criminals to serve their interests.

BYOD

Bring Your Own Device is a company policy by which employees are allowed to bring their own devices (laptops, smartphones, tablets, etc.) to work. This type of flexibility increases the number of vulnerabilities in a company’s environment, since the devices are managed and secured individually.

Computer forensics

is the practice by which digital data is collected and analyzed for legal purposes. The conclusions can be used in the fight against cyber-crime.

Disaster Recovery Plan (DRP)

A recovery plan is a set of procedures that are meant to protect or limit potential loss in case of an online attack or major hardware or software failure.

Distributed Denial of Service (DDoS) Attacks

These attacks are usually done against governments and big businesses. Servers and websites are targeted and the attacks are accomplished by sending many requests for information.

Exploit kits

are computer programs designed to find flaws, weaknesses or mistakes in software apps (commonly known as vulnerabilities) and use them to gain access into a system or a network.

Firewall

A firewall is a network security system designed to prevent unauthorized access to public or private networks. Its purpose is to control incoming and outgoing communication based on a set of rules.

Payload

The payload contains the fundamental objective of the malware transmission, which is why the payload is actually the element of the malware that performs the malicious action.

Penetration Testing

This is a type of attack launched at a network or computer system in order to identify security vulnerabilities that can be used to gain unauthorized access to the network’s/system’s features and data. Penetration testing is used to help companies better protect themselves against cyber attacks.

Phishing

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages.

SMiShing

is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device. SMiShing is short for "SMS phishing."

Social Engineering

Tricking computer users into revealing computer security or private information, e.g. passwords, email addresses, etc., by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response.

Spoofing

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Powered by Sonic Performance Support
Hamburg, Germany

Cyber Security Awareness Training

Glossary

Spyware Threats

Spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information.

Spyware, Adware and Advertising Trojans

are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software onto your computer.

SQL and XSS Attacks

Here, the hackers will submit a special section of database query code to a particular server. The server will, in turn, disclose some sensitive information when responding with the corresponding results. This is known as an SQL and XSS injection attack.

Unsecured Wireless Access Points

If a wireless access point hasn't been secured, then anyone with a wireless device (laptop, PDA, etc.) will be able to connect to it and thereby access the Internet and all other computers on the wireless network.

Viral Web Sites

Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites, are often made to look like well-known web sites and can have similar web addresses to the sites they are imitating.

Virus

A computer virus is a program written to alter the way a computer operates without the permission or knowledge of the user.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

Powered by Sonic Performance Support
Hamburg, Germany