What is a dictionary attack?

A method used to break password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary (referred as wordlists) in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password.

Why is salt used in cryptography?

In cryptography, a salt is random data that is used as an additional input to a function that hashes a password. The primary function of salts is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks. For an example on creating account and inserting password system automatically includes "salt" to the password so it would not resemble a dictionary word.

What kind of technique is password hashing?

Hashing a password will take a clear text string and perform an algorithm on it to get a completely different value. This value will be the same every time, so you can store the hashed password in a database and check the user's entered password against the hash. Use "salt" - a bit of additional data which makes your hashes significantly more difficult to crack. Examples of hash functions are md5, SHA-1, SHA-256, GOST, HAVAL.

#

hacking

How does brute force cracking work?

A brute force attack is a trial-and-error method used to obtain information such as a user password using brute force rather than employing intellectual strategies. In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Programmer relies on the computer's processing power and tries all possible combinations starting from "a, b, c... aa, ab, ac..., aaa..." ect.

What does the Moore's Law say?

An observation made by Intel co-founder Gordon Moore in 1965. He noticed that the number of transistors per square inch on integrated circuits had doubled every year since their invention. Moore's law predicts that this trend will continue into the foreseeable future.

Currently it would take a desktop PC about 39 days to crack password "Safety4me".

Describe a good password and name 3 of the 25 most used weak passwords.

A strong password is difficult to detect by both humans and computer programs. It consists of at least 14 characters that are a combination of uppercase and lowercase letters, numbers and symbols. Strong password do not contain words that can be found in a dictionary.

Top 25 most used passwords are 123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, iloveyou, adobe123, 123123, Admin, 1234567890, letmein, photoshop, 1234, monkey, shadow, sunshine, 12345, password1, princess, azerty, trustno1, 000000.

What is card skimming and a skimmer?

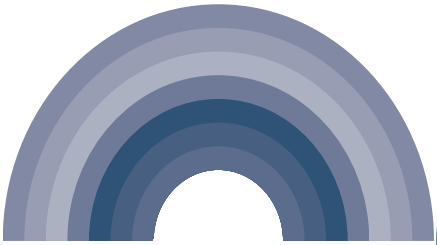
Card skimming is the illegal copying of information from the magnetic strip of a credit or ATM card using fake card slots (skimmers) and keyboard overlays or hidden camcorders for your security PIN. The scammers try to steal your details so they can access your accounts.

What are rainbow tables used for?

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

Example:

a - 0cc175b9c0f1b6a831c399e269772661
b - 92eb5ffee6ae2fec3ad71c777531578f
c - 4a8a08f09d37b73795649038408b5f33
A - 7fc56270e7a70fa81a5935b72eacbe29



hacking

What sensitive information can be dug up from an image besides the obvious?

Metadata:

EXIF info (Exchangeable image file format), a small overview thumbnail preserved even after cropping the picture;

Geotag (GPS location coordinates);

Face recognition;

Object recognition
(e.g. car number);

Camera make and model;

Date and time.

What is the difference between HTTP and HTTPS?

HTTP (Hypertext Transfer Protocol) is used by the World Wide Web. HTTP defines how messages are transmitted, and what actions Web servers and browsers should take. For example, when you enter a URL in your browser, HTTP command is sent to the Web server directing it to fetch the requested Web page.

HTTPS (HTTP Secure) makes it more difficult for hackers, the NSA, and others to track users. The protocol makes sure the data isn't being transmitted in plain-text format, which is much easier to eavesdrop on.

What is a DDoS (Distributed-Denial-of-Service) attack?

It is DoS attack conducted using multiple machines. Hacker co-ordinates the attack of "zombie machines". The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so attacker overloads the server. This is a "denial of service" because you can't access that site.

internet

What is CAPTCHA and what is it used for?

An acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart" is a type of challenge-response test used in computing to determine whether or not the user is human. The test was introduced by Alan Turing in his 1950 paper.

Using a CAPTCHA challenge during form submission significantly reduces the number of potential spam-bots on your website.

digital safety

internet

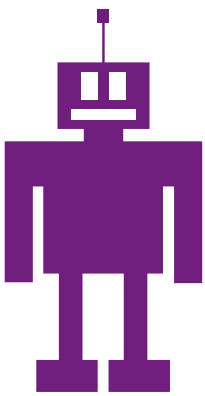
What is cyberbullying? Give an example.

Cyberbullying is bullying that takes place using electronic technology such as cell phones, computers, and tablets as well as communication tools as social media sites, text messages, chat, and websites. Examples of cyberbullying include mean text messages or e-mails, rumours sent by e-mail or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

What is a bot?

A bot (short for ”robot”) is a automated program, that performs or simulates human actions on the Internet. Web-bot is a software application that runs automated tasks over the Internet. The largest use of bots is in web spidering. Chat-bot can interact with users through chat mechanisms. Game-bots automate repetitive tasks, using them is considered cheating.

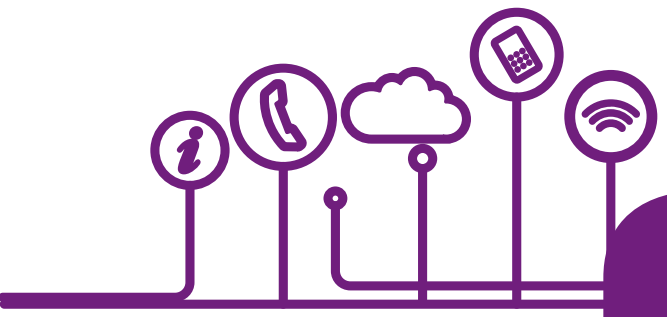
According to 2013 study 61.5% of all Web traffic is now generated by bots.



internet

What does ISP stand for?

An ISP (Internet Service Provider), is a company that provides its customers access to the internet and other web services. ISPs can vary in size - some are operated by one individual, while others are large corporations. They may also vary in scope - some only support users in a particular city, while others have regional or national capabilities.



internet

I will choose and ask you to name two of the following chat acronyms.

AFK	Away from keyboard
AKA	Also known as
BB	Bye bye
BRB	Be right back
CYA	See you!
K	Okay
GG	Good game
IRL	In real life
LOL	Laughing out loud
NP	No problem
OMG	Oh my god
RTFM	Read the f****g manual
TY	Thank you
WB	Welcome back
WTF	What the f***

What does URL stand for and what does it do?

URL (Uniform Resource Locator) is the web browser address of internet page or file. URL works together with domain names to help us name and locate webpages without the need to input hard to memorize IP addresses.

I will choose and ask you to name one of the following worldwide Internet usage fact. (+/-5%)

Note that current world population is 7.3 billion.
How many..

..people are using the Internet? (39%)

..websites content is in English? (55%)

..users use Internet in English language? (27%)

.. adult cell owners use their phones to go online? (63%).

internet

What is a botnet?

Criminals distribute malware that can turn your computer into a bot (aka zombie). Botnet is a network of private computers infected with malicious software and controlled without the owners' knowledge.

Botnets are used to send out spam e-mail messages, spread viruses, attack computers and servers with DDoS. If a computer becomes part of a botnet, computer might slow down and might be helping criminals.

malware

What is spyware?

Spyware is software that aids in gathering and sending information about a person without their knowledge. It is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Its presence is typically hidden from the user, it`s difficult to detect and it can collect user logins and bank account information. Spyware can install additional software, redirect Web browsers or change computer settings. Sometimes, it is included along with genuine software, and may originate from a malicious website.

What is a keylogger and what does it do?

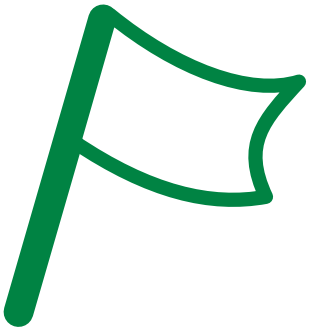
Software and hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. Software keylogger is installed and hidden to your computer. Hardware keylogger can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a keyboard and a computer. Keyloggers can automatically send data over the internet to their controller.

What is a zero-day exploit?

A zero-day is an attack that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch. It is called a "zero-day" because the programmer has had zero days to fix the flaw. It is common for individuals or companies who discover zero-day attacks to sell them to government agencies for use in cyberwarfare.

What is ransomware?

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.



malware

What is a back door?

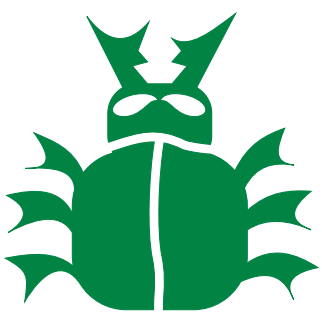
A back door is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit and gain unauthorized access to data.

404.

What is malware?

”Malware” is an umbrella term used to refer to a variety of forms of hostile software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware etc. Malware is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems

For an example fake antivirus is a malware designed to steal information by mimicking legitimate security software. It makes system modifications making it difficult to remove the program.



malware

What is payload (in computer security)?

Refers to the part of malicious code that performs the destructive operation. In the analysis of malicious software such as worms, viruses and Trojans, it refers to the software's harmful results. Although not all viruses carry a payload, a few payloads are considered extremely dangerous.

Some of the examples of payloads are data destruction, offensive messages and the delivery of spam emails through the infected user's account.

Describe a rootkit.

A rootkit as ultimate malware threat is designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Rootkit is a Trojan horse type program. It hides evidence of attackers' activities and remains is hidden. It also gives attackers remote backdoor access to the systems. Rootkit replaces normal programs and system libraries with it's own.

malware

I will choose and ask you to describe one of the following Wi-Fi glossary terms.

AP (Access Point) - A device that acts as the bridge between wireless clients and the network.

Captive Portal - AP can intercept clients who must agree to terms of service.

WPA2 (Wi-Fi Protected Access v2) - is currently the strongest encryption protocol available to wireless networks.

WPS (Wi-Fi Protected Setup) - makes it easier for users to add Wi-Fi clients to wireless networks. It is vulnerable to a brute-force attack and should be disabled.

network

What is an IP Address? Give an example.

IP (Internet protocol) address is a four-part or eight-part electronic serial number. An IP address can look something like 193.40.56.90 (IPv4) or like '2001:7d0:8240:b201:8d73:3604:38b9:2e40' (IPV6), complete with dot or colon separators. Every computer, cell phone, and device that accesses the Internet is assigned IP address for tracking purposes. Wherever you use internet actions are connected to your IP address and can be tracked back to you.

127.0.0.1
sweet
127.0.0.1

Name the three protocols that are used to deliver and receive e-mail.

IMAP (Internet Message Access Protocol) - e-mail is received and held for you by your Internet server. As this requires only a small data transfer.

POP3 (Post Office Protocol 3) - all your e-mail messages will be downloaded from the mail server to your local computer.

SMTP (Simple Mail Transfer Protocol) protocol is used to deliver your e-mail to the recipient's mail server. The SMTP protocol can only be used to send e-mails, not to receive them.

What is NFC (Near Field Communication) and how can it be used?

Technology used most often with mobile devices to exchange data based on proximity contact. NFC technology is being built into mobile phones for data transfer, touch to pay technologies, and smartcard reading.

network

What is the FTP (File Transfer Protocol) used for? Name one FTP client application.

The File Transfer Protocol (FTP) software is used to receive or send files from one computer to another. FTP is built on a client-server architecture. FTP connection can be anonymous but is commonly account based.

Popular FTP Client progams are Cyberduck, FileZilla, FireFTP, SmartFTP, Windows FTP, WinSCP, WS_FTP

What is P2P (Peer-to-peer) file sharing?

P2P is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. P2P file sharing allows users to access media files music, movies, and games using a P2P software program that searches for other connected computers on a P2P network. Example of these programs are Torrent clients, Kazaa, Emule, Soulseek.

network

What is Rogue DNS or fake DNS aka DNS hijacking?

Malware changes computer's DNS (Domain Name Servers) server to point at a rogue DNS server under the control of an attacker or through modifying the behaviour of a trusted DNS server e.g. changes website ads or blocks gambling sites. These modifications may be made for malicious purposes such as phishing, or as a form of censorship and surveillance like Great Firewall of China.

network

What is the utility ping used for?

Ping is a computer network utility used to test the reachability of a computer on an network. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an response. In the process it measures the time from transmission to reception and records any packet loss.

I will choose and ask you to name one service for one of the these ports.

21 File Transfer Protocol (FTP)

22 Secure Shell (SSH) service

23 Telnet

25 Simple Mail Transfer Protocol (SMTP)

53 Domain Name System (DNS)

80 Webserver, Hypertext Transfer Protocol (HTTP)

443 Secure Hypertext Transfer Protocol (HTTPS)

993 Mail IMAP SSL

network

How can a cookie track you?

Cookie is a small text file placed on your computer when you visit a Web page. Used to remember you when you revisit that page or to track your browsing activities, cookies facilitate virtual shopping carts, page customization, and targeted advertising. Cookies are not programs and cannot read your hard drive or cause damage to your computer.

Tracking cookies are not harmful like malware, worms, or viruses, but they can be a privacy concern.

Describe the difference between dark internet and darknet.

A dark Internet refers network hosts on the Internet that no-one can reach. According to some estimates, only 0,03% of the web is searchable, hence leaving 99,97% of all data being dark Internet. The data on the dark Internet is generally harmless in nature, being kept off the internet simply because it is data which most people won't need or search for anyway.

Deep web or darknet is distributed filesharing, which refer to hard-to-find websites and secretive networks that span the Internet.

What is a BCC (blind carbon copy)? Name some reasons for using it.

BCC allows you to hide recipients in e-mail messages. There are a few main reasons for using BCC:

Privacy - If sending e-mail on behalf of an organization, it is important to keep lists of clients confidential.

Tracking - you want to make someone, such as a supervisor or team member, aware of the e-mail.

Respect for your recipients - People often forward e-mail without removing the addresses of previous recipients. Spammers may collect and target those addresses.

privacy

What is FinFisher (aka FinSpy) and who uses it?

FinFisher or FinSpy is a piece of computer spyware designed to allow law enforcement to spy on a computer or mobile phone. FinFisher malware is installed in various ways, including fake software updates, e-mails with fake attachments, and security flaws in popular software.

FinSpy backdoors have been found in a total of 25 countries. Including Australia, Canada, Czech Republic, Estonia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Netherlands, Serbia, Singapore, United Kingdom, United States.

privacy

What steps can you take to avoid having compromising photos of you published online?

Do not take pictures of yourself in any compromising position. Don't get photographed in compromising positions when partying. Do not post, send or upload intimate pictures onto any website.

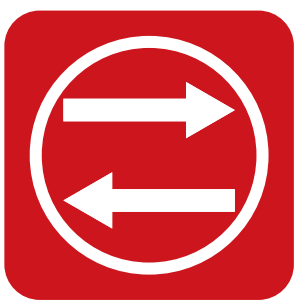
Always try to imagine your loved ones or employers viewing this image. If someone takes a private picture of you ask them to delete it. Friendships relationships are not always forever. Disgruntled friends are often posting undesirable images.

How does identity theft happen?

Someone pretends to be someone else by assuming that person's identity, to gain access to resources in that person's name. The victim of identity theft can suffer consequences if they are held responsible for the perpetrator's actions. Criminal may be able to impersonate you to purchase items, open new accounts, or apply for loans. Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available.

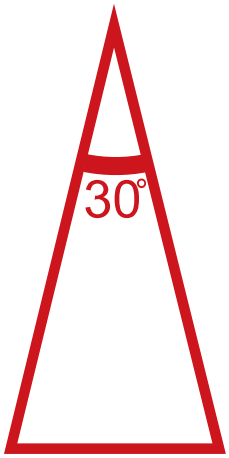
What is a proxy server?

A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. Today, most proxies are web proxies, facilitating access to Internet and providing anonymity.



What is the PRISM (a surveillance program)?

PRISM is a electronic surveillance data mining program known to have been operated by the United States National Security Agency (NSA) since 2007. Its existence leaked by NSA contractor Edward Snowden. The Prism program collects stored Internet communications based on demands made to Internet companies such as Google Inc. It's predecessor was ECHELON at Menwith Hill.

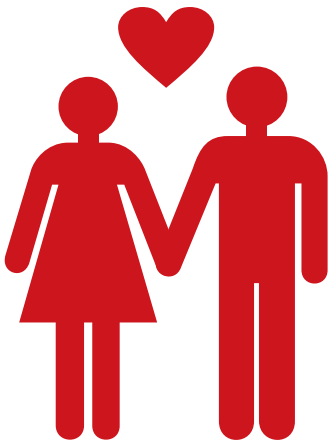


privacy

What is sexting and why is it dangerous?

Sexting (sex and texting) is the act of sending sexually explicit messages or photographs, usually between mobile phones.

Social danger with sexting is that material can be very easily and widely propagated, over which the originator has no control therefore sexting can ruin one's reputation.



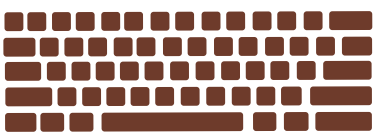
What is social engineering?

Social Engineering as a threat to most secured networks is hacker's multiple stages clever manipulation of the natural human tendency to trust. Hacker uses technology based and human based conscious techniques to get victim (without them knowing) performing actions or divulging confidential information. Using technical skills to obtain information or physical access will allow him/her to gain unauthorized access to a valued system and eventually access organization's resources or assets, including information, information systems, or financial systems.

social engineering

Describe typosquatting. Give and example.

Typosquatting, also called URL hijacking or fake url relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to fake URL. Examples of this would be:
a common misspelling: exemple.com;
a misspelling based on typing errors: xample.com or examlpe.com;
a differently phrased domain name: examples.com;
a different top-level domain: example.org.



What is spam? Describe example content of spam.

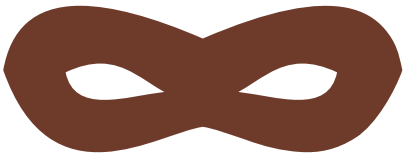
E-mail spam is unsolicited e-mail, usually sent in bulk to a large number of random accounts to people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services, phishing scams. Spam can be minimized using e-mail filtering software.

One spaming technique is e-mail spoofing – when a spammer sends out emails using your email address in the "From:" field to make it seem like the message is from you – in order to trick people into opening it.

What is pretexting (in social engineering)?

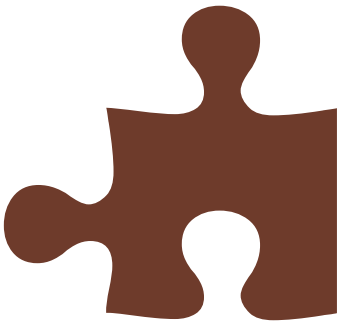
Pretexting can be used to impersonate co-workers, police, IT helpdesk etc. who could have authority in the mind of the targeted victim. Often all that's needed is a authoritative voice.

In "Quid pro quo" pretexting technique the attacker calls random numbers at a company claiming to be calling from technical support. The attacker will "help" solve a problem and eeventually they will hit someone with a legitimate problem. They guide the user to type commands that give the attacker access or launch malware.



Describe how XSS (Cross-Site Scripting) works.

Attacker exploits a vulnerability in a website that the victim visits by injecting a client-side script that executes malicious JavaScript in another user's browser. As an example attacker inserts javascript in a comments box that redirects to malicious website.



social engineering

What is baiting (in social engineering)?

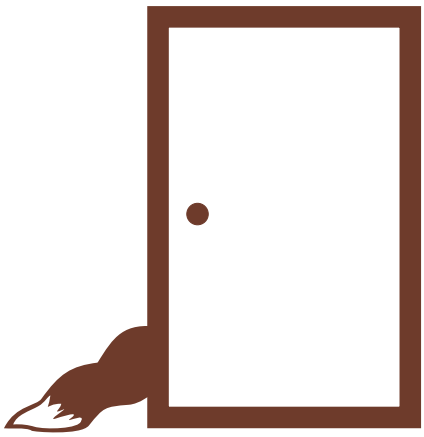
Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim. As an example an attacker leaves a malware infected USB flash drive in a location sure to be found and waits for the victim to use the device. Inserting the media into a computer to see the contents, the user would unknowingly install malware on it.

What is dumpster diving?

Practice of sifting through commercial or residential trash to find items (passwords, network information) that have been discarded by their owners, but that may prove useful. This is a powerful tactic because it is protected by social taboos. Trash is bad, and once it goes into the trash, something is best forgotten. And remember that locks can be unlocked.

How does tailgating work (in social engineering)?

In security, tailgating or piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area. E.g. slip in a door after someone, joining a large crowd authorized to enter. It can be regarded as one of the simpler forms of social engineering.

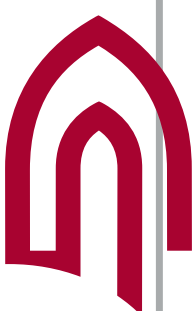


Describe how criminals use phishing.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy e-mail or website. For an example defaced Paypal, typosquatted facepook.com.

The trick usually arrives in the form of an email message that appears to come from a valid company. The message often looks like the company's website. This is called "spoofing". The message tries to convince you that you must "verify" your personal information and re-enter your account inormation.

social engineering



TALLINN UNIVERSITY

Digital Safety Lab