Glossary Of Terms

This is an updated glossary based on our years in Sunbelt Software as an antivirus developer, and in KnowBe4 as largest worldwide platform in the security awareness training and simulated phishing space. We are sharing it here as a resource. Each letter starts with acronyms in alphabetical order, then full words. (last updated Aug 26, 2023)

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

A

ACH

Automatic Clearing House, companies that do Electronic Funds Transfers. There is a tremendous amount of cybercrime and fraud connected to this area.

ACL

Access Control List. Access Control is a system or technique for allowing or denying access. Passwords and other types of ID are access controls. In Windows, an access control list (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

ACV

network security. A server running Active Directory is called a domain controller. AD authenticates and authorizes all users, computers and software in a Windows network—assigning and enforcing security policies for all computers and installing or updating software. See Wikipedia. If you want to have your own software communicate with Active Directory, you use the so called "Lightweight Directory Access Protocol" (See LDAP futher below). In our case, we want to communicate with our customer's AD (using LDAP) to synchronize changes in new users and people leaving the company with the database of users on our side so that there is much less or no user management left to do for the system admin at our customer.

One other word related to Active Directory is "OU" or "Organizational Unit" since we allow our users to specify what they want to synchronize by both security group and OU. Here is a good definition: An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure.

AI - Generative and Predictive

A fancy term for when we teach machines to *mimic* human thinking. While predictive AI is focused on analyzing data and making predictions about future events, generative AI is focused on creating new content based on existing data. Both tools have the potential to transform an industry by optimizing events, creating personalized experiences, and for instance driving customer loyalty. Also, both can be used for bad purposes.

AITM

Attacker In The Middle. A tactic where session cookies are stolen using a proxy and the bad actor gets control over the connection.

AUP

Acceptable Use Policy. A policy that defines the actions that network users are allowed to perform. Used both inside private organizations, ISPs and public entities like libraries.

AV

In our world, short for Antivirus, not (Audio/Visual). A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

information in their own application, or sometimes for data analysis. In the plainest terms, an API is a blueprint that enables "your stuff" to talk to and work with "their stuff." See Wikipedia.

APT

Short: Advanced Persistent Threat (APT) refers to prolonged, stealthy attacks that are generally difficult to detect and may go on for many months before they are discovered. An APT is a threat that is targeted, persistent, evasive and advanced. A key difference between most malware and an APT is the ATP's ability to persist — that is, to evade detection by network security controls while still collecting and extracting data.

Long: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, etc.). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Artifacting

The emergence of visible or audible anomalies, created during the process or transmission of digital data such as photographs or video graphics (applies to the subject of deepfakes)

Astroturfing

Astroturfing is *the use of fake grassroots efforts* that primarily focus on influencing public opinion and typically are funded by corporations and governmental entities to form opinions.

ASLR

Address Space Layout Randomization. A security feature in the Windows OS which randomly assigns executable code to 256 potential RAM locations, trying to protect against buffer overflow attacks.

Access Controls

exploit the accounts they need to covertly access systems with sensitive data. The attacker leverages his appropriated access to appear like a legitimate user on the network.

ActiveX

The brand name of a group of Microsoft technologies that allow for special additional features in HTML. You implement ActiveX with "controls", but using these can open the door to hackers as it makes the attack surface a lot bigger.

Advance-fee fraud

A type of scam in which a cybercriminal persuades a potential victim to help transfer a substantial amount of money to an account. The victim is offered a commission for facilitating the transaction or multiple transactions. Many Nigerian scams, also called the 419 scam, are a prime example of advance-fee fraud.

Adware

Adware is any software which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive, and can be used by cyber criminals to steal confidential information.

Agile Software Development

Fast and flexible software development methodology that is used by KnowBe4 for rapid development of our products. See Wikipedia.

Algorithm

A *set of rules* to be followed in problem-solving operations. You can use algorithms for practically any kind of computer debugging or handling malware. Here is a YouTube example of a very popular encryption algorithm: SHA-256.

Angler Phishing

Angler phishing is the practice of masquerading as a customer service account on social media, hoping to reach a disgruntled consumer.

Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies. See Wikipedia.

Anti-phishing filtering

Phishing is the process in which bad actors try to trick you into giving out sensitive information or taking a potentially dangerous action, like clicking on a link or downloading an infected attachment. They do this using emails disguised as contacts or organizations you trust so that you react without thinking first. It is a form of criminally fraudulent social engineering. Anti-phishing products help filter unwanted phishing attempts from reaching your inbox. They are never perfect.

Anti-spam filtering

Like with physical mail, users may get a lot of unwanted mail. With e-mail, this is called spam. Anti-spam filtering works by analyzing incoming emails for red flags that signal spam or phishing / malicious content and then automatically quarantining them to a different email folder.

Anti-Tampering

Software and other security measures which make it harder for attackers to modify software/systems.

Anti-Spyware Coalition (ASC)

The Anti-Spyware Coalition (ASC) is a group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies.

Attack surface

The “attack surface” of a software environment is all the points (the “attack vectors”) where an attacker can try to penetrate the network. More at Wikipedia. An organization’s “phishing attack surface” is all the email addresses of that domain that can be found by the bad guys.

Attack vector

access the network.

AV-test.org

An organization in Germany run by Andreas Marx, which provides independent antivirus testing for AV Vendors and for magazines like PCWorld. They are here.

Awareness Definition

- knowledge or *perception of a situation or fact* (Google)
- having or *showing realization, perception*, or knowledge (Merriam-Webster)
- knowledge or understanding of something; *ability to notice things* (Macmillan)

B

BEC

Short for Business Email Compromise, which is also known as CEO Fraud. Also See EAC and VEC.

BIC

The FBI has coined a this "deepfake attack vector" name: Business Identity Compromise, it is BEC on steroids.

BGP

Border Gateway Protocol. BGP is often likened to a GPS navigation service for the internet, enabling infrastructure players to swiftly and automatically determine routes for sending and receiving data across the complex digital topography. And like your favorite GPS mapping tool, BGP has quirks and flaws that don't usually cause problems, but can occasionally land you in major traffic jams.

BGP hijack

for those targets flow through the malicious ISP's network, where it can sniff its content or carry out Man-in-the-Middle attacks. For instance, this really happened. all traffic for Washington DC was routed to China for a few hours. Guess who was sniffing the data...

BHO

Browser Helper Object. Designed by Microsoft with the best of intentions, BHO's were intended as 'plug-ins' to add functionality (like toolbars) to Internet Explorer. Unfortunately, malware authors have also exploited the power of BHO's for other purposes such as spreading malware.

BYOD

Bring Your Own Device. It's your network, but it's their personal device, either a phone, tablet or laptop. What could go wrong? Mobile devices are a fabulous way for hackers to penetrate the network using social engineering techniques. Mobile device security has not kept up with mobile device malware and if hackers can infect a mobile device, it's an easy way to hack into the network.

Baiting

Baiting means dangling something in front of a victim so that they take action. It can be through a peer-to-peer or social networking site in the form of a (porn) movie download or it can be a USB drive labeled "Q1 Layoff Plan" left out in a public place for the victim to find. Once the device is used or malicious file is downloaded, the victim's computer is infected allowing the criminal to take over the network.

Backdoor

A backdoor in a PC is a method of bypassing normal authentication, obtaining remote access to a PC, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or malware could modify existing software on the PC creating a backdoor that way. Here is an overview of the threat types, categories and their descriptions:

Backlog

Term from Agile software development. Also called 'Sprint Backlog'. It is a list of items left to be done. See 'Agile', 'Burndown', and 'Sprint'.

Backup

competitor combined with the strengths of our own product.

Banker Trojan

Banker Trojans, designed to steal financial information entered into browser-based online forms are the cybercriminals' answer to the crackdown on keylogging. In addition to snatching form input, Banker Trojans are also designed to trick users into visiting web sites designed to look authentic. Once there, users are prompted for personal information causing identity theft.

Bayesian filtering

An old-ish statistical method mainly used as a baseline to filter out spam which does not work very well. The bad guys have found many ways around it.

Behavioral Analytics

Behavioral analytics studies people's reactions and behavior patterns in particular situations. Behavioral analytics is often used for business opportunities, but the techniques are just as applicable to identify and alert on risks. Behavioral analytics is used in banking for fraud detection, and helps gaming systems to identify cheaters. Behavior analytics is a broad application of data science, machine learning, and AI techniques. More at infoWorld.

Behavioral Detections

Antivirus detects malware using signatures, heuristics and behavior. The behavior-based method varies by product.

Behavioral Economics

Behavioral economics studies the effects of psychological, cognitive, emotional, cultural and social factors on the decisions of individuals and institutions. It wasn't until 1970 that behavioral economics came of age thanks to the work of Israeli social scientists, Nobel Prize winning economist, Daniel Kahneman and Amos Tversky. Kahneman and Tversky found significant evidence that humans, in certain circumstances, show a systematic pattern of deviation from the norm or rational judgment.

Beta Testing

Testing performed by a group of customers in a live application of the software, at one or more end user sites, in an environment not controlled by the developer.

Blacklist/black list/block list

A list of known bad files, bad domains or bad email addresses you do not want mail from. The first two are blocked by Antivirus when the user tries to access them. Bad email addresses (senders) can be blocked in a variety of ways. Also see Whitelist.

Blended Malware

Malware often contains more than one malicious technology. It can have the characteristics of a worm, but use virus technology to infect other machines, and behave like a Trojan. The malicious code is a blend of technologies. This is the thing that system administrators fear the most, by survey.

Bloatware

Software that takes a lot of CPU and Memory resources while running on the computer. Antivirus companies have been adding more and more code over the years to protect against increasingly sophisticated malware. But they are using LOTS of CPU and RAM to do it, and so system admins call these traditional AV vendors as creating 'bloatware'.

Bogus Redirection

A process that captures traffic addressed to a legitimate website and sends (redirects) it to a different website instead. Some malware does automatic redirection to fool users into thinking they're interacting with a valid and legitimate site rather than a malicious one.

Boot Virus

A virus that infects the Master Boot Record (MBR) of a hard disk drive.

Buffer overflow

Also called "buffer overrun". Simplified, it's a case of sloppy coding which allows an attacker to write data to a memory buffer, overruns that buffer's boundary, and overwrites the memory next to it with executable code that they can then use to hack into the system.

A more technical explanation is as follows: In computer security, a buffer overrun, or buffer overflow, is an unwanted condition where a process stores data in a memory buffer outside the memory the programmer set aside for it. This extra data overwrites adjacent memory, which may result in a variety of

Burndown

A term used in 'agile' software development, a method that KnowBe4 uses. The burndown chart is a publicly displayed chart showing remaining work in the sprint backlog. Updated every day, it gives a simple view of the sprint progress. It also provides quick visualizations for reference. See 'Scrum', and 'Sprint'.

Bot, spam bot, ddos bot

Software, owned and controlled by the bad guys, that lives on infected PCs and runs autonomously. See 'Botnet' and 'DDOS'.

Botnet, also called 'Bot army'

Botnet is a jargon term for a collection of software robots, or 'bots', that live on infected PCs and run autonomously. While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities. Botnets do many bad things, like spew out spam, attack other PCs or web servers, or send back confidential data to the botnet command-and-control (C&C) servers. They are managed by a "Bot Herder"

Bot Herder

The bad guy, who attacks other systems with the botnet(s) that he owns.

Browser Hijacker

A malicious piece of software that changes the web browser's settings without the permission of the user. Examples: change the Home page to another site, changes the search engine default page and other activities, generally attempting to force hits to a certain website to boost that site's advertising revenue.

Brute force attack

A Brute Force Attack is a relatively simple, automated method to gain access to a system. The brute force software tries usernames and passwords, over and over again, until it gets in. It's not very sophisticated, but when users have passwords like '123456' and usernames like 'admin', it's very effective. They are an attack on the weakest link in IT security: the user.

C&C server aka "C2" server

Command & Control Server used to run botnets. See ‘Botnet’.

CaaS

Cybercrime-as-a-Service.

CVE

The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known information-security vulnerabilities and exposures. The United States' National Cybersecurity FFRDC, operated by The Mitre Corporation, maintains the system, with funding from the US National Cyber Security Division of the US Department of Homeland Security.[1] The system was officially launched for the public in September 1999.[2] The Security Content Automation Protocol uses CVE, and CVE IDs are listed on Mitre's system as well as in the US National Vulnerability Database.[3] More at WIKIPEDIA

CASB (Cloud Access Security Broker)

Cloud Access Security Broker (CASB) serves as a tool for enforcing an organization's security policies through risk identification and regulation compliance whenever it's cloud-residing data is accessed.

CARA

Compliance Audit Readiness Assessment. CARA is a free tool that helps you gauge your organization’s readiness in meeting compliance requirements for the CMMC.

CEO Fraud

Spear phishing attacks focusing on people in Accounting, claiming they are the CEO and to urgently transfer large amounts of money. CEO fraud is a form of social engineering that took flight during 2015.

CDSBA

California Database Security Breach Act. CA State law which requires disclosure to CA residents if their PII or PHI has been stolen or is believed to have been stolen (See PII and/or PHI). If more than 500 records are stolen, lawyers almost immediately file a class-action lawsuit.

No, not the Langley guys. Information Security term meaning **C**onfidentiality, **I**ntegrity, and **A**vailability. It is a model designed to guide policies for information security within an organization. Confidentiality is a set of rules that limits access to information. Integrity is the assurance that the information is relevant, accurate and trustworthy. Availability is a guarantee of ready access to the information by authorized people.

CIA versus KGB

There are quite a few books about these intelligence agencies, and it would take a very long time to read. Luckily, here is an article with the short history of both the CIA and the KGB.

Cloud-based Antivirus

Cloud-based antivirus solutions are those that store information about malware in the cloud, rather than on a user's device. Antivirus is software designed to detect and destroy computer viruses.

CISO

Chief Information Security Officer

CSO

Chief Security Officer

CMMC

Cybersecurity Maturity Model Certification (CMMC) framework, required by the US Department of Defense (DoD),

COPPA

Children's Online Privacy Protection Act. A U.S. Federal Law that requires owners of social media sites and websites directed at children under 13 to get parental consent before the site collects and uses the child's personal information.

Catfishing

companies are called channel partners or often just for short: 'The Channel"

Chain (as in full chain exploit or full exploit chain)

Exploit chains (also known as vulnerability chains) are **cyberattacks that group together multiple exploits to compromise a target**. Cybercriminals use them to breach a device or system to greater success or impact compared to focusing on a single point of entry. More.

Ciphertext

Data that has been encrypted and cannot be read by a human, as opposed to cleartext.

Cleartext

Data that has not been encrypted and can be read by a human, as opposed to cyphertext. Sending credit card data over the Internet in cleartext is an invitation to disaster. Storing confidential information on hard disk without encrypting it is making a hacker's life easy.

Clickbait

En eyecatching link or controversial story on a website which encourages people to read on. Can also be used to get users to click on links to malware.

Cloud computing

The name 'cloud computing' was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams. It means using applications that live on the Internet instead of on your PC or your corporate server. SalesForce.com is a good example, but there are many others. The advantage is that someone else takes care of the hardware and software, (for a fee). There are different categories of cloud computing, here are a few: Software as a Service (SaaS), Utility Computing, and Managed Service Providers (MSP).

Cloud-based

A computing model where a company does not have its own servers, but rents server space in large datacenters. KnowBe4 lives in the Amazon cloud.

Code Complete

modified by anyone else. Antivirus companies use this for whitelisting of good applications by the company that signed the application, for example DELL, Microsoft, Apple, etc. They also use this for blacklisting all applications from certain companies like known to create unwanted software.

Cognitive Bias

Cognitive biases are systematic errors in human thinking and decision making (Tversky & Kahneman, 1974). Exploited by social engineering, but is also the cause of bad business decisions. Great article here. And there is a very useful KnowBe4 blog post by Perry Carpenter with useful links here.

Company Extinction Event (CEE)

A bug so severe that it would cripple the service you provide so bad, that it would kill the whole company. For instance, antivirus are very powerful engines, so it has the power to bite very hard and make a brick out of people's workstations instantly, by the millions. It almost happens now and then to most antivirus companies who regularly dodge bullets like this.

Compatibility Testing

The process of determining the ability of two or more systems to exchange information. In a situation where the developed software replaces an already working program, an investigation should be conducted to assess possible comparability problems between the new software and other programs or systems.

Compliance

The action or fact of complying with a wish or command. From "comply" – act in accordance with a wish or command. From Latin "complire" – to fill or fulfill.

A compliance report is a report to the originator of an order that the order has been done and is a completed cycle. When a compliance officer receives a "done" as a single statement without any evidence, noncompliance can slip through. That is why every compliance report must be accompanied with evidence that shows the cycle is indeed a real *"done".* or at the very least an attestation from the Directly Responsible Individual that the task has been completed.

In the context of KnowBe4 Compliance Manager it means having an (IT) environment that is up to the standards of the regulations of that industry one is in. Many industries are regulated by one law or another and need to comply with that law, for instance HIPAA for Health Care organizations, Sarbanes-

ubiquitous part of everyday life.

Computer Forensics

Forensic Science dealing with legal evidence found in computers and digital storage media. Computer forensics is also known as digital forensics. It's simply using special software tools to search for and preserve evidence of a crime. See Wikipedia.

Conficker

Also known as Downup, Downadup and Kido, is a computer worm targeting the Windows operating system, and was first detected in November 2008. It uses flaws in Windows software to make PCs into zombies and link them into a botnet that can be commanded remotely by its criminal owners. Conficker at its peak had more than seven million computers under its control. The worm uses a combination of advanced malware techniques which has made it difficult to counter, and has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer. Antivirus catches and quarantines Conficker, but we have to keep on top of this one, as it is being run by very smart bad guys.

Container

A simplified look at a container is a set of processes that are isolated from the rest of the system. All the files necessary to run a container are provided from a distinct image. This means that containers are portable and consistent as they move from development, to testing, and finally to production, and you can quickly get a new AWS instance up & running. Here is a sysadmin guide to containers.

Content Filtering

Content filtering is a process that manages or screens access to specific emails or webpages. The goal is to block any content that contains harmful information. It is never perfect because it is mostly reactive. Content filtering products allow you to prevent access to harmful and malicious content and websites while still providing your employees access to good, appropriate, and relative information. Unrestricted internet access can lead to inappropriate, malicious, or harmful content.

Cookie

In its basic form, a short line of text that a web site puts on your computer's hard drive when you access that web site. That way when you return, that web site knows you were there before and can automate

The sudden and complete failure of a computer system or component.

Credential-stuffing attacks

In which hackers rapidly test email and password combinations at a given site or service. These are typically automated processes that prey especially on people who reuse passwords across multiple sites on the internet. Here is an article.

Crimeware

Malware intended to steal money from an individual or financial institution. Culture wars are about topics like politics, education, religion, abortion. Often they are fought with misinformation, disinformation and manipulation of the facts.

Culture War

Culture wars are battles over what a nation values. They tend to heat up whenever there is change in society.

Cybercrime

The term Cyber- or Computer crime encompass a broad range of potentially illegal activities. In KnowBe4's context, we mean crimes that target computer networks or devices and their users directly. A few examples out of many more possible:

- Malware, including viruses
- Denial-of-service attacks via Botnets
- Spear phishing scams, resulting in identity theft, data breaches and other major damage.

Cybercrime Attack Map

Kaspersky has a live map that shows all cyber attacks going on in real time. You can see it here.

Cyberheist

Organized crime penetrating the network of an organization and emptying their bank accounts via the Internet. Also the title of a book by KnowBe4's CEO Stu Sjouwerman for executives of enterprises explaining the dangers of cybercrime. See this.

D

DAC

Data Access Control

DACH

Short for the combination of german-speaking countries Germany, Austria, and Switzerland.

DDoS

A distributed denial of service attack (DDoS). A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Done in various ways, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all.

DDR

Data Detection & Response

DEP

Data Execution Prevention. A security feature in the Windows OS which tries to prevent hackers from using buffer overflow attacks.

DHCP

Dynamic Host Control Protocol. It's a standardized protocol that dynamically provides IP address assignment from a pool of available IP addresses from an ISP or a network router. A "DHCP lease" is the lease of an IP address to a network user. DHCP is part of the Internet's TCP/IP protocol suite.

protect corporate data. The systems are designed to detect and prevent the unauthorized use and transmission of confidential information. See Wikipedia.

DMARC

Domain-based Message Authentication, Reporting and Conformance (**DMARC**) is an email-validation system designed to detect and prevent email spoofing. ... **DMARC** is built on top of two existing mechanisms, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). See Wikipedia.

DMR

Direct Market Reseller, also known as an e-tailer which is a company that sells directly to consumers online without operating storefront operations of any kind.

DMZ

Demilitarized Zone. A separate computer host or even a small network placed as a “neutral zone” between an organization’s secure private network and the outside insecure Internet. The DMZ does two things: 1) prevents outside users from getting direct access to a system which has confidential information, and 2) provides Internet access to users in that organization.

DNS

Domain Name System: It's is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. In very simple terms, it translates domain names like www.example.com to a number like 93.184.216.34 that corresponds with a computer on the internet somewhere.

DNS Hijacking

DNS hijacking, also known as silent server swaps, is a malicious attack vector that can be used to forcibly redirect web traffic to websites that are either fake or different from the ones you’ve requested. Here is a blog post that explains DNS Hijacking.

DPI

Deep Packet Inspection. A form of computer network packet filtering. DPI is performed as the packet passes an inspection point, searching for non-compliance, viruses, spam, intrusions or predefined criteria to decide what actions to take on the packet, including collecting statistical information. This is in contrast

Database-protections

Database security refers to the various measures organizations take to ensure their databases are protected from internal and external threats. Database security includes protecting the database itself, the data it contains, its database management system, and the various applications that access it.

Data Breach

A data breach is the intentional or unintentional release of secure information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill. More at Wikipedia

Data-driven Defense

A data-driven computer security defense will help any entity better focus on the right threats and defenses. It will create an environment which will help you recognize emerging threats sooner, communicate those threats faster, and defend far more efficiently.

Data Lake

Data Lakes are different than data warehouses. Big Data takes in large volumes of data from multiple sources and pours it into one data lake. The information sits unfiltered, unprocessed and unstructured. Security analytics tools like Looker can extract knowledge from the data lake via machine learning to expose patterns and insights.

Data Science

Data Science is the application of math, big data analytics and machine learning to extract knowledge and detect patterns. It is an emergent technology area in the realm of cybersecurity, used in many areas.

Deal Registration

A channel partner (See **Channel**) does not like to do a lot of marketing and then lose their deal to someone else. The way to prevent this is registering a deal through the channel partner portal where the channel partner can make sure they are protected and get their deal.

Decryption

The process of changing (encrypted) ciphertext back into cleartext.

Defense-in-Depth

Defense in Depth is a security discipline that protects all six levels of an IT infrastructure. including policies, procedures & awareness, perimeter, internal network, host, application and data.

DevSecOps

DevSecOps is short for development, security, and operations. An extension of the devops model for software development, it involves applying security measures throughout the software development life cycle (SDLC). DevSecOps calls for everyone involved in the development process to be aware of the need for security. As a model, DevSecOps encompasses a set of practices to increase collaboration between the security, development, and operations teams, with the goal of making software more secure. More at InfoWorld

Dictionary Attack

An automated attack on a password that uses common words from dictionaries and compares these to the password being attacked. If you use a common word from a dictionary as your (very weak) password it's an invitation to be hacked.

Digital Certificate

A digital stamp or electronic document that verifies the identity of a person or organization. The certificate includes a very secure password issued by a reputable certificate authority, such as VeriSign or Thawte.

Disinfection

Cleaning up a PC that is infected with malware. Disinfection can be done automatically by Antivirus, but sometimes needs to be done manually by our Security Response Team.

Disinformation

False information which is intended to mislead, especially propaganda issued by a government organization to a rival power or the media. These are also called influence campaigns or manipulation campaigns. Disinformation is often forwarded to friends and family and at that point it is called *misinformation*. Russia invented disinformation under the leadership of Joseph Stalin who created a special agency that took propaganda campaigns to w shole new level called Dezinformatsiya.

The way in which something is placed or arranged, especially in relation to other things. For PhishER, we mean taking "unknown" emails and arranging them into "clean/spam/threat".

DNS Server

Domain Name System (DNS) servers map a human-recognizable identifier (e.g. www.KnowBe4software.com) to a computer-recognizable numeric identification (e.g. 64.128.133.188 which is KnowBe4's Terminal Services machine). See Wikipedia.

Domain Admin

A Domain Administrator is basically a user authorized to make changes to global policies that impact all the computers and users connected to that Active Directory organization.

Domain Controller

A domain controller is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing access to resources in that domain. It authenticates users, stores user account information and enforces security policy for a domain. Wikipedia

Domain Spoof Test (DST)

A service that KnowBe4 provides, which sends an email to a prospect that is spoofed to come from their own domain. This is not supposed to be able to get through to them. Their mail server needs to be configured so that these emails from the outside that have an inside email address are deleted. Request a free DST here.

Doppelgänger (Domain)

Is an "evil twin" domain that looks very much like your own domain but is malicious. It uses *punycode* (see below) and *homographs* (see below) to deceive the end-user they are clicking on a legit domain. bad guys are using punycode and homographs to create domains that look almost identical to the original. KnowBe4 has a free tool you can run to see if your domain has evil twins. It's called Domain Doppelgänger and you can find it here.

Downloader, also Rogue Downloader

Drive-by-download, also called Drive-by-install

Something bad got installed on a user's PC without their knowledge or consent. It is a transfer of software from a web server to an unsuspecting user's computer. It occurs in the background, with no notification, when a user visits a particular web page. A user need only access the web page to be subject to the download. Such downloads usually include malware when some kind of scam or attack is under way. The expression is used in four increasingly strict technical meanings. See Wikipedia for those.

Dumpster diving

Dumpster diving involves looking in the trash for any valuable information, like data written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information.

E

EAC

EAC is short for Email Account Compromise, a close relative of BEC. The primary difference is with EAC, criminals target individuals rather than businesses to initiate fraudulent wire transfers.

EDR

Endpoint Detection and Response (also see XDR)

EFT

Electronic Funds Transfer

EEC

The EICAR virus (pronounced eye-car) was developed as a sample virus that is used in the IT security industry to see if antivirus is working. It's completely safe, it's only used to test the basic functionality of antivirus.

EOL

End Of Life. Software industry lingo meaning a product will be retired and no longer supported.

EPP

Endpoint Protection Platform. An integrated security solution designed to detect and block threats at device level.

ESG

Environment, Social and Governance. Do you know the language of ESG investing? As sustainable investing grows so do related terms and phrases. Glossary at WSJ:

ERP

ERP stands for Enterprise Resource Planning and refers to software and systems used to plan and manage all the core supply chain, manufacturing, services, financial and other processes of an organization.

EULA

End-User License Agreement. (That thing no one ever reads...) A software license agreement is a contract between the “licensor” and purchaser of the right to use computer software. The license may define ways under which the copy can be used, in addition to the automatic rights of the buyer. Many EULAs are only presented to a user as a click-through where the user must “accept” and is then allowed to install the software.

Email Antivirus Scanning

Scanning enterprise email for antivirus can be done in four (!) different spots.

- At an email hosting company, where enterprise email is outsourced
- At the perimeter by a dedicated gateway product

true meaning. The science of encrypting and decrypting information is called cryptography. The original text, known as plaintext, is converted into an unreadable form known as ciphertext. When an authorized user needs to read the data, they may decrypt the data using a key or password. This will convert ciphertext back to plaintext so that the user can access the original information.

Endpoint

Another word for the workstation that is used by an end-user in an organization. Refers to a computer or device at the end of a network cable. The PC you are reading this from is called an 'endpoint' by system administrators. Symantec calls their corporate antivirus Symantec Endpoint Protection (SEP).

Enrich [PhishER]

Improve or enhance the quality or value of. When adding additional data about reported emails we are giving the admin more at a glance information about what they are looking at, thus we are *enriching* the messages.

Ethics Policy

A policy created for employees in an organization which is supposed to be a guide and a reference for said employees that helps them make day-to-day decisions which are "the greatest good for the greatest number". Also known as a "Code of Ethics". As opposed to "Acceptable Use Policy" which is more like a Moral Code with hard "survival" rules about do's and dont's to keep the organization alive.

Exchange

Short for 'Microsoft Exchange Server' which handles corporate email (and more). There are Antivirus Security Products for Exchange which protect the Exchange server against viruses and spam. MS-Exchange is out there in five versions, 2003, 2007, 2010, 2012 and 2014.

Exfiltration of Data

Data Exfiltration is often of of the end goals of cyber criminals. It's the unauthorized transfer of data from a computer by malware and/or a malicious actor (also called data theft).

Exploit, sometimes called zero-day exploit

An exploit (French, meaning "achievement") is (usually malicious) software that takes advantage of a bug, glitch or vulnerability in other code in order to cause unintended or unanticipated behavior to occur, and

stages of a cyber attack, because they have the ability to download malicious files and feed the attacked system with malicious code after infiltrating it. Example: The owner of A PC with old versions of Flash and the Firefox browser was social engineered to go to a legit but compromised website. The EK discovered the old software versions, looked in its database of known vulnerabilties, and used exploits to take over the PC and infect it with ransomware.

F

419 Scam

Scams originating from Nigeria are called 419 scams as the number “419” refers to the article of the Nigerian Criminal Code dealing with fraud. Most of the scams are very old, have been used earlier with fax and snail mail, and are now used on the Internet. There is a whole industry in Nigeria around these scams.

FIDO

FIDO stands for **F**ast **ID** **O**nline. It's an alliance that tries to overcome the major problems with passwords.

Fake News

Fake news is the promotion and propagation of news articles via social media. These articles are promoted in such a way that they appear to be spread by other users, as opposed to being paid-for advertising. The news stories distributed are designed to influence or manipulate users’ opinions on a certain topic towards certain objectives.

Feature Flags

Feature flags are a software development concept that allow you to enable or disable a feature without modifying the source code or requiring a redeploy.

FP

False Positive. In the antivirus world this means a file is flagged as malicious (and possibly quarantined) when it isn't. This can cause the computer to malfunction. In the antispam world an FP means that a legit email was flagged as spam and quarantined.

File Sharing Protections

Secure file sharing is the process of sharing one or more files securely or privately. It enables sharing files between different users/organizations confidentially and/or within a protected mode, secure from intruders or unauthorized users. Secure file sharing is also known as protected file sharing.

Feature Complete

A product build is called feature complete when the product team agrees that functional requirements of the system are met and no new features will be put into the release, but significant software bugs may still exist. This happens at the Beta stage in the Software Development Life Cycle (SDLC).

Firewall

Short: A device or software product that can block attacks by filtering data packets.

Long: A firewall is designed to block unauthorized access while permitting authorized communications. Either hardware or software, it is configured to permit or deny all (in and out) computer traffic based upon a set of rules and other criteria. There are several types of firewalls. See Wikipedia. In KnowBe4 we use the term 'human firewall' to indicate all users are trained to a point where they do not fall for any social engineering tricks.

Flashing

The process you use to rewrite the contents of EPROM like the BIOS. An EPROM is a read-only memory chip whose contents can be erased and reprogrammed.

Framing

Framing has been defined as information and experiences in life that alter the way one reacts to the decisions one must make. From a nonsocial engineer point of view, framing is your own personal

fraud analytics uses advanced algorithms to correlate cross-channel activities related to user, account, device, location and business transactions.

Forensics

In our context, “digital forensic science” that deals with legal evidence found in computers and digital storage media. The goal is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting evidence of a cybercrime.

Foundational Model (AI)

The term “foundation model,” introduced last year by a team of Stanford researchers, refers to a massive AI model trained on broad swaths of data that, rather than being built for a specific task, can perform effectively on a wide range of different activities.

G

GLBA

The Gramm-Leach-Bliley Act (GLBA, pronounced “glibba”), also known as the Financial Modernization Act of 1999, is a U.S. federal law that requires banks and financial institutions to protect private information of individuals.

GRC

Governance, risk and compliance (*GRC*) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Think of *GRC* as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements.

Gamification

Manipulate (someone) by psychological means into questioning their own sanity. "in the first episode, Karen Valentine is being gaslighted by her husband"

Gateway

Device or software that is between the internal network and the external network.

Graymail

1) Graymail is *solicited bulk email messages that don't fit the definition of* email spam (e.g., the recipient "opted into" receiving them). Wikipedia

2) Graymail is *the threatened revelation of state secrets in order to manipulate legal proceedings*. It is distinct from blackmail. It is a tactic used by the defense in a spy trial, involving the threat to expose government secrets unless charges against the defendant are dropped. Wikipedia

Grey IT

Employees in the organization installing and implementing technology without going through normal channels, getting no approval, and no IT and/or InfoSec buy-in. It is not allowed as per the KnowBe4 Acceptable Use Policy.

Governance

In essence, governance is a system of checks and balances to ensure that managers make decisions in the interest of the corporation. Think of it as the organizational choices about how everyone involved is going to “play the game.” This includes agreeing to what the company is trying to achieve (its mission and objectives), the steps it is going to take to get there (strategy and operational business choices) and how to ensure outcomes are achieved and managers are held accountable (board oversight and executive compensation). More at WSJ

Greyware

A Potentially Unwanted Program, also called “PUP”.

Have I Been Pwned. The name of a service run by Troy Hunt, where you can check if your credentials are part of a data breach. Some KnowBe4 tools like Password Exposure Test integrate with this site.

HIPAA

The Health Insurance Portability and Accountability Act, was enacted by the United States Congress and signed by President Bill Clinton in 1996. It requires healthcare organizations to protect personal health information. (See PHI)

HIPS

Host Intrusion Prevention System. Intrusion prevention systems (IPS) are a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. See Wikipedia

HDR

Human Detection and Response. Combining KnowBe4's leading platform for security awareness training and simulated phishing testing with real-time behavior analysis and micro-learning results in the creation of a new cybersecurity category called "Human Detection and Response (HDR)". See Press Release

HTTPS

In computing, a communication protocol refers to the set of rules that computers use to communicate with each other. (HTTP) Hypertext Transfer Protocol is used for accessing and receiving (HTML) files on the internet. A more secure version of HTTP is called HTTPS (Hypertext Transfer Protocol Secure). This contains https:// at the beginning of the URL. It encrypts all the information that is sent and received. This can stop malicious users such as hackers from stealing the information and is often used on payment websites. It is not a cure-all. There are many way to get around it.

Hacker

Originally: A person who has advanced computer skills, is enthusiastic and skillful. If they attack computers it is not done with malicious intent. Recently though the definition has changed and means anyone who illegally breaks into or tries to break into networks and/or computers.

Ham

encrypted) passwords and other secrets (SSH Keys, DevOps secrets, etc.) into the source code.

Heuristics

Heuristic comes from the Greek for “find” or “discover”. They are experience-based techniques that help in problem solving. Heuristics are “rules of thumb”, or educated guesses. Antivirus uses heuristics in the form of dynamic pattern assessment to determine if a code sample is malware.

Heuristic Detections

Antivirus detects malware using signatures, heuristics and behavior.

Homograph:

A term used to describe when two or more characters have shapes that are similar or identical. A simple example is the number zero and a capital letter "o", it's easy to confuse an O a 0.

Honeyclient

These are like honeypots, but instead of lying totally dormant, they emulate user’s surfing behavior and can catch malware that way.

Honeydoc

A file on a PC or server that sits equipped with a beacon, waiting to be stolen and then calls home to tell its owner where it is and who stole it.

Honeypot

A PC that sits, unprotected, on the Internet waiting to get infected through the FTP and HTTP threat vectors.

Honeytrap

A social engineering trick that makes men interact with a fictitious attractive female online. From old spy tactics where a real female was used.

Hotfix

Human Firewall

With our information systems under aggressive attack, we cannot ignore *any* layer of the defense-in-depth model. The human element of cyber security is too often overlooked. Workforce cyber preparedness is urgently needed. Security Awareness Training can pay off by training users on what they can do to prevent malicious activity and what to do in the event of such activity. It helps people to see their identity as an important part of keeping their organization secure and that what they do matters.

Hijacker, also called 'Homepage hijacking'

Spyware that changes the default homepage someone has, to a site that displays ads, a different search engine, or worse, porn. They are very hard to get rid of for the average consumer.

IC3

The FBI's Internet Crime Complaint Center. They are here.

IAB

Initial Access Brokers. IABs are threat actors who sell access to malicious services and play a crucial role in the ransomware-as-a-service economy. IABs facilitate network intrusions by selling remote access to a computer in a compromised organization and link opportunistic campaigns with targeted attacks, often ransomware operators. IABs don't undertake ransomware attacks but sell access to a compromised network that is then used by ransomware gangs and others. More here.

ICSA Labs

ICSA Labs provides vendor-neutral testing and certification for security products and solutions. Here they are.

IDS

Intrusion Detection System. An Intrusion detection system (IDS) is a network security device (or software) that monitors network and/or system activities for malicious or unwanted behavior. Also see 'HIPS'

IoC

Indicators of compromise (oOCs) are "pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network." Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threats.

ISP

Internet Service Provider.

ItW

In The Wild. ItW is the name for malware that is supposed to be out there in the wild. Opposed to the 'Wildlist' which is the official CURRENT actual list. That list can change every month. Something that is on the Wildlist is ALWAYS ItW but something that is ItW listed doesn't necessarily have to be in the actual Wildlist.

Identity Theft

Taking someone else's Social Security Number, Address and other important personal information to establish false credentials and commit fraud. A good example is the creation of fraudulent credit card accounts, racking up charges which are then left unpaid, leaving the identity theft victim with the credit card debt and a ruined credit rating.

Incident Response (IR)

In the event that the security of a system has been compromised, a quick incident response is necessary. It is the responsibility of the security team to respond to the problem quickly and effectively. An example would be a security team's actions against a hacker who has penetrated a firewall and is currently sniffing internal network traffic. The incident is the breach of security. The response depends upon how the security team reacts, what they do to minimize damages, and when they restore resources, all while attempting to guarantee data integrity. (See Forensics).

Information Security

Input validation

Input validation prevents malicious or poorly qualified/formatted data from entering an information system by using a technique that rejects or accepts data based on a set of rules. This is used to ensure only properly formed data is entering the system.

Insider Threat

A threat that organizations face from within their own networks. They are difficult to detect and stop because insiders already have access to sensitive information and know how to retrieve it. Conventional perimeter security and rules-based security tools cannot stop the insider threat because insiders are not a known threat. The insider threat can be current employees, former employees, or third-party vendors and contractors. Insider threats can be either malicious or accidental. More.

Integrity checks

An IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted.

J

JSON

Once upon a time there was one computer. Then someone built a second one and wanted some code off the first computer. That meant we needed a way to move information without dependencies on the underlying hardware. Since then, there have been many character encoding and interchange standards (ASCII, EBCIDIC, SGML, XML, etc.) that have had their time in the spotlight. For the past few years, JavaScript Object Notation (JSON) has been the most popular. More.

Java

A programming language specifically created to add features to HTML pages. Note that JavaScript is different from Java.

K

Kevin David Mitnick (1963 - 2023)

During the mid-nineties, Kevin Mitnick was the 'World's Most Wanted Hacker', and became a very successful Fortune 500 Security Consultant: Based on his 30+ years of first-hand experience with hacking and social engineering, KnowBe4 created its New-school Security Awareness Training. Kevin died peacefully on Sunday, July 16, 2023, at age 59 after valiantly battling pancreatic cancer for more than a year. Kevin is survived by his beloved wife, Kimberley Mitnick, who remained by his side throughout their 14-month ordeal.

Kernel Level

The foundation of the Operating System is called the Kernel. It provides basic, low-level services like hardware-software interaction and memory management. If a product works at the kernel level, this has many advantages.

Keylogger aka Keystroke logger

A form of malware or device that observes what someone types on their keyboard and sends this data back to the bad guys. There are several ways to do this, using either software or hardware.

KnowBe4 Product Abbreviations

Kevin Mitnick Security Awareness Training = KMSAT (with year indication)

KnowBe4 Compliance Manager = KCM GRC Platform

take a closer look at their network and understand how to recognize and defend at various points along a hacker's methodology.

L

LAMP

LAMP is a software bundle, assembled to make an open source web platform consisting of Linux, Apache, MySQL and Perl/PHP/Python.

LDAP

Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard protocol to access and maintain directory information services like Active Directory. If you want to have your own software communicate with Active Directory, you use the so called "Lightweight Directory Access Protocol" (See Wikipedia).

LLM

A Large Language Model (LLM) is a type of artificial intelligence that understands and generates human-like text. It learns from vast amounts of data, enabling it to answer questions, write essays, and engage in conversations with users.

LMS

A Learning Management System (LMS) is software for the administration, documentation, tracking, reporting and delivery of e-learning education courses or training programs. Organizations can have their own LMS in-house or use a cloud-based LMS like Knowbe4 provides.

Laserphishing

Q4 2009, as the first antivirus company ever, Sunbelt Software began to offer VIPRE Antivirus as a “PC Lifetime Subscription” via the Home Shopping Network. Priced at $99.95, Sunbelt calculated the average lifetime of a PC to be four to five years. Other AV companies started this type of subscription in following years.

Linux

An extremely popular open-source Unix operating system variant. It comes in many flavors.

Log Aggregation

The practice of consolidating log files throughout the IT infrastructure into a centralized platform for the purpose of organizing the log data for review and analysis. It’s a key step in the process of producing insights into application and device security.

Logic Bomb

A malicious computer program (or part of a program) that is asleep until it gets woken up by a specific logical event. Examples are pieces of code hidden by Chinese military hackers in a U.S. power plant that can disable the plant at a certain time. An example of this is a sleeper ransomware strain that infected workstations but only woke up at a certain time.

M

MASA

Multi-Factor Authentication Security Assessment. KnowBe4’s new Multi-Factor Authentication Security Assessment (MASA) is a complimentary IT security tool that helps you gauge your organization's MFA security readiness and identifies your specific risks so you can better defend against MFA hacks.

MBR

MEME

1) An element or "unit of culture" of transmission that may be considered to be passed from one individual to another.
2) A humorous image, video, piece of text, etc., that is copied (often with slight variations) and spread rapidly by Internet users. From Greek mimēma ‘that which is imitated’, on the pattern of gene .

MSP

A Managed Service Provider (MSP) is a company that manages information technology services for other companies via the Web.

MSSP

A managed security service provider (**MSSP**) is an IT service provider that provides an organization with agreed upon levels of cybersecurity monitoring and management, which may include virus and spam blocking, intrusion detection, firewalls and virtual private network (VPN) management.

MTBF

Mean TIme Between Failure. Short for mean time between failures, the average time a device will function before failing. MTBF ratings are measured in hours and indicate the sturdiness of hard disk drives and printers. Typical disk drives for personal computers have MTBF ratings of about 500,000 hours. This means that of all the drives tested, one failure occurred every 500,000 hours of testing. See Webopedia for more.

Machine Learning

Think of it simply as a branch of statistics, designed for a world of big data. The most common application of machine learning tools is to make predictions. Here are a few examples of prediction problems in a business. Good article here.

- Making personalized recommendations for customers
- Giving a score if an email is clean, spam, or a threat
- Forecasting long-term customer loyalty
- Anticipating the future performance of employees
- Rating the credit risk of loan applicants

Macro

Malicious Attachment blocking

Malicious email attachments are designed to launch an attack on a user's computer. The attachments within these malicious emails can be disguised as documents, PDFs, e-files, and/or voicemails. Actions taken to block/prevent attachments like these are used to protect both the mail system and individual mailboxes from those malicious software.

Malware

Malware is a shorter version of the term “Malicious Software”. It is an umbrella term used to refer to a wide range of viruses, worms, Trojans and other programs that a hacker can use to damage, steal from, or take control of endpoints and servers. Most malware is installed without the infected person ever realizing it.

Malware-blocking

Tools that can help block malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer.

Malware and Malicious Action Blocking

Also called Malware Behavior Blocking. It provides a layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time. As programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. This type of software can ensure a higher level of protection against new, unknown, and emerging threats, and is often driven by machine learning and AI.

Maintenance aka Renewal

The period that a customer gets tech support, updates and new software versions.

Malvertising

Malvertising is malicious advertising that contains active scripts designed to download malware or force unwanted content onto your computer. Exploits in Adobe PDF and Flash are the most common methods used in malvertisements. See ‘Exploit’.

Malware protection

Internet. See Cloud Computing.

Man-in-the-middle attack

An attack in which data sent and received between two parties in an ongoing connection is intercepted. The attacker can record, read, or even alter the contents of that traffic.

Mean-time-to-detect

Mean-time-to-detect (MTTD) is the average length of time it takes a cybersecurity team to discover incidents in their environment. The lower an organization's MTTD, the more likely they'll be to limit any damage done by a cyber incident.

Media Drop

Technique used by hackers who load malware on a USB drive, CD/DVD, or other readable form of media, and then leave the infected media where it can easily be found. In some cases, thieves actually give the media away at public venues or trade shows. Once the victim loads the drive or disk, the malware does its work and will allow the hacker to do a number of things, including take remote control of the victim’s computer.

Metadata

Relatively abstract data about other data. Example: records of what cell phone number calls what other number at what time. There are many different kinds of metadata.

Metamorphic Virus

Typical polymorphic malware will only rewrite part of its computer code to evade detection. Metamorphic malware goes even further by completely recompiling its code during each infection when it first connects to the internet.

Middleware

Middleware is software that exists between an operating system or database and the applications running on it, especially on a network or in a distributed environment. It enables data management and communications between the OS and applications by functioning as a hidden translation layer.

Milware

contexts, but that core concept is very, very similar to the *very intentional focusing-on-the-present-moment mindset* that we hope employees adopt to suss out phishing attacks and to, well, be mindful of the threats all around them. If you're familiar with Daniel Kahneman's System 1 and System 2 thinking model, there's definitely a linkage between mindfulness and finding ways to intentionally enter System 2." See below for definitions of System 1 and System 2 thinking. PS, here is an interesting article: "How AI neural networks show that the mind is not the brain."

Misinformation

False or inaccurate information, especially that which is deliberately intended to deceive. Often forwarded to friends and family, not knowing it is false. See Disinformation.

Money Mules

A person recruited by a criminal or criminal organization to quickly receive and turn around funds involved in scams. The scams are often related to ACH, credit cards, or similar online transactions. The money mule is often unaware of his or her actual role.

Multi-factor authentication

A method of validating the identity of a user by using two or more security mechanisms. For example, a valid user name and password combination along with a fingerprint scan is a form of multi-factor authentication. Modern cybercrime has developed malware to evade some forms of multi-factor authentication.

N

NADM

Never **A** **D**ull **M**oment. The motto of the business we are in.

Network Attached Storage. A network hardware technology that uses a strand-alone storage device that is dedicated to centralized disk storage.

NAC

Network Access Control. A piece of technology that controls access to a network. See Wikipedia

NAP

Network Access Protection is a Microsoft technology for controlling network access of a computer host based on the system health of that computer. With NAP, system admins can define policies for system health requirements. I.e. are the most recent operating system updates installed? Are the anti-virus software definitions updated? Has that computer a firewall installed and enabled? You get the idea. Computers not in compliance with system health requirements have restricted or no access to the network.

NCSAM

National Cyber Security Awareness Month

NFC

Near-field communication (NFC) is a set of communication protocols that
enables communication between two electronic devices over a distance of 4 cm (1½ in) or less. Your phone communicates to your Yubikey using NFC. More at Wikipedia

NGAV (Next Generation Antivirus)

An endpoint is any device that connects to a computer network like your phone or laptop. Next-Generation Antivirus (NGAV) uses new technologies to protect endpoints in a way that is fundamentally different from traditional antivirus by using advanced technologies, to look for patterns of behavior used by attackers.

NIC

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network

NW3C

Network Device Logs

A log is a running record of everything that is constantly happening on a website or in a system. It contains various data points e.g., timestamps with user actions like, "John Smith clicked on the training tab at 09:00 AM EST". Network Log files capture things like unsuccessful log-in attempts, failed user authentication, or an unexpected amount of requests on your servers, all of which can signal to an analyst that a cyber attack might be in progress. The best security monitoring tools can send alerts and automate responses as soon as these events are detected on the network.

Network Firewall

A Network Firewall is a security device used to prevent or limit illegal access to private networks. It uses policies that define what data is allowed on the network; any other data seeking to connect to the private network is blocked.

Network Traffic Analysis (NTA)

NTA applies behavioral analysis to network traffic to detect suspicious activities that traditional cybersecurity tools miss. Network traffic analysis continuously analyzes raw network traffic using machine learning and artificial intelligence. When abnormal network traffic patterns are detected an alert is raised and the threat can be mitigated.

NIPS

Network Intrusion Prevention System. Intrusion prevention systems (IPS) are a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. See Wikipedia

NIST

The National Institute of Standards and Technology (NIST) has an excellent publication with templates and guides for what should go into a security awareness training program. The 70-page document is available for free in PDF format from the institute's Web site. Here is a site that explains the NIST Cybersecurity Framework in "plain English"

14th-century Franciscan friar William of Ockham "Occam's Razor" cuts through complexity with a no-nonsense approach. in short: all else being equal, simplicity is best. So is this actually true? Is the simplest explanation usually the best one? Not exactly. Ockham never said complexity is inherently inferior to simplicity, nor did he declare complex explanations inherently wrong. Complex scientific questions often demand complex answers, and that's not at odds with Occam's razor. The principle merely states that unnecessary complexity is, well, unnecessary. "Occam's razor is about finding the simplest solution that works," Johnjoe McFadden.

Ockham was not the first to promote simplicity. Aristotle held that "the more limited, if adequate, is always preferable," and Ptolemy considered it best "to explain phenomena by the simplest hypothesis possible." Some three centuries after the genesis of Occam's razor, Isaac Newton would declare that "we are to admit no more causes of natural things than such as are both true and sufficient to explain their appearances." About 200 years after that, Albert Einstein would agree that "everything should be made as simple as possible, but not simpler"

When used correctly, Occam's razor works. If two computer programs accomplish the same task, the one with less code is inevitably more efficient. MORE

OEM

Original Equipment Manufacturer. An OEM manufactures products or components which are purchased by another company and retailed under the purchasing company’s brand name. OEM refers to the company that originally manufactured the product. See Wikipedia.

ON-ACCESS Scanning

Malware scans that are monitoring the system in real-time for any changes and will prevent immediate infection.

ON-DEMAND Scanning, also called ‘drive scan’

Malware scans that are set to run on a scheduled basis, like 3am every night.

OPSEC

OPSEC (operations security) is a security and risk management process and strategy that classifies information, then determines what is required to protect sensitive information and prevent it from

positive psychological benefits, such as increased motivation, but it can also lead to unrealistic planning and decision-making.

ORGANIZATIONAL UNIT (OU)

A word related to Active Directory is "OU" or "Organizational Unit" since we allow our users to specify what they want to synchronize by both security group and OU. Here is a good definition: An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure. See Active Directory "AD".

OS and Application Event Log

A log is a running record of everything that is constantly happening on a website or in a system. It contains various data points e.g., timestamps with user actions like, "John Smith clicked on the training tab at 09:00 AM EST". An Application Log is created when an event takes place inside an application. These logs help software developers understand and measure how applications are behaving during development and before release. Logs are also needed to track network intrusions and respond to attacks.

P

PAM

Privileged Access Management (PAM) is an information security (infosec) mechanism that *safeguards identities with special access or capabilities beyond regular users*. Like all other infosec solutions, PAM works through a combination of people, processes and technology.

P/E Ratio

to equal the cost of the investment. More here.

P2P

Peer-To-Peer software allows end-users to up- and download software (movies, music, games) via a distributed computing architecture, not using centralized servers. There is a significant risk as child porn is also moving through these networks, and can result in SWAT teams busting down your door if a neighbor illegally piggybacks on your Wi-Fi. (no joke).

PCI

Payment Card Industry

PCI Security Standards Council

Organization that publishes standards (rules) on how to securely handle credit card processing.

PCI-DSS

The PCI Data Security Standard – a document published by the Payment Card Industry; it lists all the requirements for securely handling credit cards and credit card information. Organizations that accept credit cards need to be PCI compliant. This includes Security Awareness Training and many other requirements.

PHI

Protected Health Information. PHI is all recorded information about an identifiable individual that relates to that person's health, health care history, provision of health care to an individual, or payment to health care. The U.S. Health Insurance Portability and Accountability Act (HIPAA) governs the protection of Private Health Information

PII

Personally Identifiable Information. PII is defined as any instance of an individual's first name or first initial, plus the last name, and any more than thirty additional confidential items. If it can be used to uniquely identify a specific individual using non-public information, it's PII and must be protected.

Planning Fallacy (The)

Product Manager. A product manager researches, selects, develops, and places a company's products, performing the activity of product management.

PMD

Pretty Much Done. One of our old colleagues' favorite expressions, and indicated that the final product might still be months away from completion. 

POP

Period of Performance. How long the customer has paid for maintenance on their product.

Private Equity (101 glossary)

Private equity is capital invested in companies not listed on a stock exchange or publicly traded. Private equity funds buy public and private companies with the goal of increasing their value over a number of years before selling them. List of terms at Investopedia

PSD

Product Services Delivery. The team, part of the Accounting Department, that processes orders and does Roll-Out calls for KnowBe4 Products with the customers. PSD also refers to the in-house process that routes orders from quote acceptance through the delivery process.

PST

Phishing Security Test. This is a simulated phishing attack done by KnowBe4 on email addresses that a prospect or customer upload to our site. We have dozens of templates that existing customers can use on their employees. You can do a one-time free PST to all your employees

Password Dump

Also called Credential dump, which is actually a popular technique whereby an attacker scours a compromised computer for credentials in order to move laterally and/or carry out further attacks. More.

Password Hashing

Password hashing is defined as putting a password through a hashing algorithm (bcrypt, SHA, etc) to turn plaintext into an unintelligible series of numbers and letters. More.

A patch is software (security) update intended to repair a vulnerability that was discovered after the product was released for general use. The process of patching is fixing security vulnerabilities and other bugs, with such patches usually being called bugfixes or bug fixes. There is a whole category of products that do patching. See Vulnerability Management.

Patch Tuesday

Patch Tuesday is the second Tuesday of each month, the day on which Microsoft releases security patches. That week, system administrators need to do the testing of these patches in their own environments and then deploy the patches which usually requires a reboot. Sometimes systems are mission critical and cannot be rebooted, which causes them to stay vulnerable and then get infected with a zero-day threat.

Payload

Malware often comes in different parts. That is where the term 'blended malware' originates. An example is an email claiming to be from the 'Better Business Bureau' having a complaint for you about your company. Attached is a PDF. The PDF is the payload and has malware in it, or downloads malware from a compromised server somewhere. Here is a bit of history of the word and where it came from.

Peer-to-peer

See P2P

Penetration Testing

A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. (*Not to be confused with a vulnerability assessment)*. Wikipedia

Performance Testing

(IEEE) Functional testing conducted to evaluate the compliance of a system or component with specified performance requirements.

Perimeter (security)

Perimeter security refers to routers, firewalls, and intrusion detection systems implemented to tightly control access to networks from outside sources. More Here

A KnowBe4 product for managing potentially malicious email messages reported by users. Key features include: prioritization, disposition, automated workflows, automated responses, SIEM integration, data enrichment.

Phishing

Phishing is the process in which bad guys try to trick you into giving out sensitive information or taking a potentially dangerous action, like clicking on a link or downloading an infected attachment. They do this using emails disguised as contacts or organizations you trust so that you react without thinking first. It's a form of criminally fraudulent social engineering. Also see Spear Phishing.

Phishing Attack Surface

Are you aware that many of the email addresses of your organization are exposed on the Internet and easy to find for cybercriminals? With these addresses they can launch spear phishing attacks on your organization. This type of attack is very hard to defend against, unless your users get next-generation security awareness training. IT Security specialists call it your 'phishing attack surface'. The more email addresses that are exposed, the bigger your attack footprint is, and the higher the risk. It's often a surprise how many of your addresses are actually out there, whose, and where they were found. Here is a datasheet with some more information.

Phrase techniques

Methods of producing strong passwords. One technique involves creative transformations for a sentence so that, for example, "I never eat rye bread" becomes iN3V3RtaeWRYdearb

Phreaking

A form of fraud that involves directly hacking telecommunications systems, one of the things Kevin Mitnick used to do in the early days.

Plaintext

Also known as cleartext and is used as input for encryption.

Point-of-failure Training

Polymorphism

A feature of a programming language that allows routines to use variables of different types at different times. Here is where this word comes from:

- Poly = many: polygon = many-sided, polystyrene = many styrenes [(a)], polyglot = many languages, and so on.
- Morph = change or form: morphology = study of biological form, Morpheus = the Greek god of dreams able to take any form.

Polymorphic threat

Malware, spam or phishing attacks that change themselves very frequently to try to prevent detection by filters.

Polymorphic virus

Malware that shape-shifts to avoid detection by encrypting parts of its own content differently all the time.

Policy

A set of rules that specify what requirements must be met.

PowerShell

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS. More.

POP

Post Office Protocol, the email protocol that handles incoming email.

Popup

Small web browser Window that literally pops up over the browser window you are looking at. Our training uses this technology to present the user with their training session so they need to turn popup

that same amount in the future. In other words, money received in the future is not worth as much as an equal amount received today. Receiving $1,000 today is worth more than $1,000 five years from now. Why? An investor can invest the $1,000 today and presumably earn a rate of return over the next five years. Present value takes into account any interest rate an investment might earn." (and we are not even talking about inflation...)

Pretexting

The act of creating an invented scenario in order to persuade a targeted victim to release information or perform some action. Pretexting can also be used to impersonate people in certain jobs and roles, such as technical support or law enforcement, to obtain information. It usually takes some back-and-forth dialogue either through email, text or the phone. It is focused on acquiring information directly from the actions taken by the targets, who are usually in HR or Finance.

Principle of least privilege

Giving users the least amount of access required for them to complete their jobs. Also referred to as separation of duties.

Prioritize [PhishER]

Determine the order of dealing with a series of items according to their relative importance. Different organizations have a different idea of priority; some might think digging into threats is priority #1, others might feel that responding to end users letting know that PO they reported is *not* a threat is more important. In either case it's important to get rid of the junk that doesn't matter so the important items are addressable.

Privacy Policy

A privacy policy is a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer's data. There is a lot of background data about this on Wikipedia.

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Product-led growth

Propaganda

Information, especially of a biased or misleading nature, used to promote or publicize a particular political cause or point of view. Interestingly enough, although it has a negative connotation today, it has ostensibly noble origins. In 1622 in an effort to spread Christianity around the world, Pope Gregory XV established in Rome the Sacred Congregation of the Propagation of the Faith, to be entrusted to a handpicked group of cardinals. Just an example of how the meaning of words can radically change over time.

PROM

Programmable Read Only Memory. A computer chip with content that can be re-written from the outside.

Protocol

In short, a set of standards to get a specific function done. Example: TCP/IP.

Proxy server

A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. Mostly used in the context of using a proxy server to connect to the Internet. See Wikipedia.

Punycode

SHORT: The name of the technology used when a domain name uses language-specific characters. A significant portion of computing systems only expect to see and use Latin characters. When you start introducing fancy letters there has to be an a way to tell the system "get ready, these letters are going to be fancy". Punycode is how that is done.

LONG: The global Domain Name System (DNS), is responsible for turning human-friendly server names into computer-friendly network numbers, but it's restricted to the limited subset of ASCII characters in domain names. The curiously-named system known as *punycode* is a way of converting words that can't be written in ASCII, such as the Ancient Greek phrase `ΓΝΩΘΙΣΕΑΥΤΟΝ` (know yourself), into an ASCII encoding, like this: `xn--mxadglfwep7amk6b`.

Some letters in the Roman alphabet are the same shape (if not always the same sound) as letters in the Greek, Cyrillic and other alphabets, such as the letters I, E, A, Y, T, O and N in the example above. So you

In hacker jargon, ‘pwn’ means to compromise or control, specifically another computer (server or PC), web site, gateway device, or application. (it’s ‘own’ with a typo in it) It is synonymous with one of the definitions of hacking or cracking. The Pwnie Awards are awarded by a group of security researchers.

Q

QA

Quality Assurance. In KnowBe4 the team that is responsible to find bugs in our code and work with Development to deliver world-class quality to our customers.

QBR

Quarterly Business Review. A meeting of a company’s execs to determine strategy.

Quality Control

The operational techniques and procedures used to achieve quality requirements. This is typically handled during the development process.

Quarantine

Antivirus, after it detects malware, can move that malware to a protected space on disk where it cannot do any further harm, and from where it can either be deleted or restored in case it was a false positive. See ‘False Positive’.

RDP Remote Desktop Protocol (**RDP**) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

RBL

RBL stands for Realtime Blackhole Listing. RBLs are used for Antivirus Exchange and Antivirus Gateway. It's a list of domains that are blocked because they are a source of spam. You can find a complete definition of RBL at Webopedia.

RMA

Return Materials Authorization. As in: "Shipments without a valid RMA number will not be accepted."

RSN

'Real Soon Now'. A technical term that software developers use to indicate when they expect to deliver shippable code. Also see **PMD**.

RTM

Released To Manufacturing. The day that the final code is shipped out the door to the factory to be duplicated. In KnowBe4's case, the day that we released the final product on our website.

RAP Testing

Virus Bulletin is the world's most prestigious antivirus lab. Apart from their VB100 certification, they have another interesting test called RAP. It's for "Reactive and Proactive", and helps you form an impression of the heuristic -and- generic proactive detection capability of security software products – in particular how well products perform against malware that appears after vendors have submitted their products to Virus Bulletin for testing. They create a quadrant a few times a year, and compare all products they have tested. The antivirus industry is not promoting this website, as it's not a pretty picture.

The RAP system measures simple static detection rates, testing against common malware samples first seen by the VB lab team within ten days of running each stage of the test.

The "*Reactive*" measure is the average of three test runs against samples seen in the ten days before the test date, allowing the products to use the latest updates and with full access to any cloud-based

supplement client-side technologies.

Rainbow Tables

A password attack that uses a really large set of of hashes that were generated from almost every possible password.

RanSim

RanSim stands for "Ransomware Simulator". KnowBe4 released a free tool in October 2016 that people can download to check if their antivirus/endpoint protection is effective against ransomware infections. It takes several scenarios and emulates the things that real ransomware would do in a non-destructive way. You can find RanSim here.

Ransomware

Ransomware denies access to a device or files until a ransom has been paid. Also called Cryptoware. Ransomware for PC's is malware that gets installed on a user's workstation using a social engineering attack where the user gets tricked in clicking on a link, opening an attachment, or clicking on malvertising.

Once the malware is on the machine, it starts to encrypt all data files it can find on the PC itself and on any network shares the PC has access to. Next, when a user wants to access one of these files they are blocked and the system admin finds two files in the directory that indicate the files are taken ransom, and how to pay the ransom to decrypt the files. There are a number of free ransomware decryptors available, however it's a constant battle with hackers then upgrading strains to get past decryption methods. There are many strains of ransomware, two infamous ones are CryptoLocker and CryptoWall. Many more exist and new ransomware strains are released regularly.

Real Time Protection

Protecting a PC as it happens, as opposed to a scheduled scan that is done every 24 hours. See 'Active Protection, 'On Access protection.

Red Team and Blue Team

Both red teams and blue teams work toward improving an organization's security, but they do so differently. A red team plays the role of the attacker by trying to find vulnerabilities and break through cybersecurity defenses. A blue team defends against attacks and responds to incidents when they occur.

Used mainly in the IT space to indicate that a customer extends their subscription for another year.

Remote Console

System Administrators often manage several geographically dispersed sites. In those cases, they need software to be able to manage the remote site as if they were physically present. For that, they use what is called a 'remote console'. For instance, a remote console allows them to manage a machine or a whole network when they are in New York and the physical network being managed is in Atlanta.

Removal

Deleting malware from a PC. See 'Disinfection'.

Reporting

In the context of KnowBe4, reporting means the section of the cloud back-end where customers can see which employees have started their training, finished it or have not even started it. Also which Phishing security tests were sent, who opened, who clicked and a host of other data related to this.

Resident Virus

Malware that is loaded in random access memory and is able to interrupt an Operating System function and alter it to do damage.

Reverse Engineering

To disassemble and examine some code in detail to discover how and what the creator, so it can be replicated or killed.

Rogue, also Rogue Scanner, rogue anti-spyware, rogue anti-malware or scareware

Rogue security software is a form of computer malware that deceives or misleads users into paying for the fake or simulated removal of malware. Rogue security software, in recent years, has become a growing and serious security threat in desktop computing. It is a very popular social engineering tactic and there are literally dozens of these programs.

Root

Router

A router is hardware used to connect two or more computers (or other devices) to each other, and usually to the Internet, by wire or sometimes radio signals.

Ruby on Rails

Often shortened to Rails or RoR, is an open source web application framework for the Ruby programming language. It is intended to be used with an Agile development methodology that is used by KnowBe4 for rapid development.

S

SAC

Short for the **S**ecurity **A**wareness **C**ompany, which was acquired by KnowBe4 in 2017.

SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). What that jargon means is that you can use one set of credentials to log into many different websites. It's much simpler to manage one login per user than it is to manage separate logins to email, customer relationship management (CRM) software, Active Directory, etc. More.

SAQ

'Self Assessment Questionnaire'. A form that merchants which accept credit cards complete to evaluate their compliance with PCI SCC rules. There are different SAQs, depending on the way(s) in which the merchant processes transactions and the transaction volume.

the cloud directly to the employee or device. The link is to Wikipedia which goes into *much* more detail.

SAT

Security Awareness Training. To be aware, you need to be able to face things as they really are (confront). KnowBe4 helps employees face the fact bad guys are trying to trick them. Once employees realise this is actual reality, they become aware and able to detect these scam emails and can take appropriate action like deleting the email or not clicking a link. More at Wikipedia [ISAT]

SCRUM

Here is a short article that explains the difference between Scrum, Kanban and Agile. They are all methods to develop software.

Secure Boot

Secure Boot is a feature found in the startup software (when you turn your computer on) for your computer that's designed to ensure your computer starts safely and securely by preventing unauthorized software like malware from taking control of your PC at boot-up.

SHI

They are a DMR, a Direct Market Reseller also known as an e-tailer which is a company that sells directly to consumers online without operating storefront operations of any kind.

SIM card

A *subscriber-identity-module* or alternatively a *subscriber-identification-module* which is a small card that fits in your smartphone and secure they key and identity of the owner.

SIEM [PhishER]

Security **I**nformation and **E**vent **M**anagement. A type of software that pulls together data from multiple sources—often event log files—analyses it, and then can take some sort of action like alerts someone or make a pretty report. Some of the common SIEM platforms are Splunk, QRadar, and LogRythm. (See XDR)

SPF (Sender Policy Framework) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. See Wikipedia

SSO

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials -- for example, a name and password -- to access multiple applications. SSO can be used by enterprises, smaller organizations and individuals to ease the management of various usernames and passwords. SSO uses **SAML** to its magic.

Securable.io

A company acquired by KnowBe4 in 2017.

SCORM

Sharable Content Object Reference Model (SCORM) is a collection of Department of Defense created standards and specifications for web-based e-learning. It defines communications between client side content and a host system which is an LMS. (See LMS) KnowBe4's courseware is SCORM compliant.

SDK

Software Development Kit. A set of development tools that allows a software engineer to create an application. An Antivirus SDK allows someone to create their own antimalware software product, and pay the developer for the use of the SDK.

Session Cookie

Webpages have no memories. A user going from page to page will be treated by the website as a completely new visitor. Session cookies enable the website you are visiting to keep track of your movement from page to page so you don't get asked for the same information you've already given to the site. Cookies allow you to proceed through many pages of a site quickly and easily without having to authenticate or reprocess each new area you visit. All about cookies

Short Squeeze

A short squeeze occurs when many investors short a stock, or bet that its price will go down, and the stock's price shoots up instead.

SKU

Stock Keeping Unit. A number to specify a separate product.

SME, SMB

Small and Medium Enterprises (usually up to 500 seats). Also called SMB (Small and Medium Business) Some industry analysts go up to 1,000 seats before they call it ‘Large Enterprise’.

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for e-mail transmission, and is the #1 protocol in use today. E-mail servers and other e-mail transfer agents use SMTP to send email.

SOAR

Security **O**rchestration, **A**utomation and **R**esponse defined: a coordination of automated security tasks across connected security applications and processes. SOAR allows organizations to collect data about cybersecurity threats from multiple applications and respond to those threats without human interaction. SOAR consists of vulnerability management, incident response and security automation. (Also see XDR). "In a world of certainty, you can get resilience through automation. In a world of uncertainty, you get resilience through orchestration," information-security expert Bruce Schneier noted, during an RSA Conference keynote address in 2019. "Incident response is inherently uncertain, and that makes it hard to automate."

SOC

Security Operations Center (computing), in an organization, a centralized unit that deals with computer security issues

SOC 2

SOC 2 (SOC stands for (**S**ervice **O**rganization **C**ontrols) is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of its clients. For security-conscious businesses, SOC 2 compliance is a minimal requirement when considering a SaaS provider

SOW

Statement Of Work. A description of the work that needs to be done, and is agreed upon by the parties before the work starts.

Scareware

Scam software, often with limited or no benefit, sold to consumers via unethical marketing practices. The selling approach is designed to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user. Some forms of spyware and adware also use scareware tactics. Read more about this at Wikipedia

Script Kiddie

A relatively unskilled hacker who downloads and uses “point-and-click” attack software.

Scrum

A method intended for management of software development projects, it can also be used to run software maintenance teams, or as a general project/program management approach. KnowBe4 uses this method. See Wikipedia

Security Culture

We define Security Culture as the ideas, customs, and social behaviors influencing an organization's security. This is another way of saying that an organization is intentionally creating a space where cybersecurity is valued and emphasized.

Security policy

A written document that states how an organization plans to protect its physical assets and information.

Session hijacking

An attack method that captures the attributes of a website session from one of the parties involved (usually on the client or user end). It then takes over (hijacks) the session from the legitimate user. The attacker keeps the session going and impersonates the user.

Security Vulnerability

The term vulnerability means a weakness which allows an attacker to penetrate a network. It’s also called ‘attack surface’. A Vulnerability has three elements:

Sensitive information

Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it. NOTE: For our purposes, the words sensitive, confidential, and private all mean essentially the same thing

Sextortion

Contact a young girl on a social networking site using a fake identity, gain her trust, extract some highly personal information, and then threaten to expose her intimate exchanges if she doesn't assent to escalating demands for sexually explicit pictures or videos. Example at the FBI website

Shipstopper (Bug)

A bug found that is severe enough to stop the product from shipping.

Shoulder surfing

Shoulder surfing is a visual technique of gathering passwords by watching over a person's shoulder while they log in to the system. With some training, a hacker can observe a user log in and then use that password to gain access to the system.

Signature-Based Detection

Antivirus detects malware using signatures, heuristics and behavior. The signature-based method is built on proprietary threat information, using multiple sources for the threat definition updates.

Smishing

Phishing conducted via Short Message Service (SMS), a telephone-based text messaging service. A smishing text, for example, attempts to entice a victim into revealing personal information.

Sniffer

Jargon for packet analyzer software that looks at (sniffs) data packets in a network and shows what is inside the packets. Can be used to troubleshoot networks but also to hack into the network.

Social Engineering

Unsolicited, unwanted Email. About 90% of email that goes through the internet is spam. The other 10% is called 'ham'. (no joke)

Spear Phishing

Spear Phishing is a small, focused, targeted attack via email on a particular person or organization with the goal to penetrate their defenses. The spear-phishing attack is done after research on the target and has a specific personalized component designed to make the target do something against their own interest. Here is more about how they do it.

Spoofing

Tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet. E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Since people are much more likely to read a message from an address they know, hackers will often spoof addresses to trick the recipient into taking action they would not normally take.

Sprint

A term used in 'agile' software development, a method that KnowBe4 uses. A period of a month after which a deliverable product is ready for shipping. During this sprint, a list of items called 'backlog' is 'burned down' to completion. See 'Backlog' and 'Burndown'.

Spyware

An umbrella term for many 'families' of malicious software which send a computer user's confidential data back to (usually) cyber criminals. Some examples of spyware are Trojans, Adware, malicious toolbars, and many others. For a short history on spyware, check out this item on Wikipedia. It's not complete but gives a reasonable overview.

SQL Injection Attack

SQL injection is a hacker technique that exploits a security vulnerability occurring in the database of an application. The vulnerability is present when user input fields are not checked well.

Stateful (as in "Stateful Firewall")

viruses, spyware, and other badware. You can find them here

Stress Testing

(IEEE) Testing conducted to evaluate a system or component at or beyond the limits of its specified requirements.

Stu's Rules

KnowBe4 founder and CEO Stu Sjouwerman ends staff meetings with:

- Do it right the first time
- Do it fast
- Have fun while you do it!

Stuxnet

Malware created by the U.S and Israel with the express goal to destroy Iran's uranium enrichment facility in Natanz. It escaped and is now used by bad actors to attack sites. More Here

Switches

A switch, in the context of networking, is a device that receives data and sends it to the proper computer on a local area network (LAN).

Supply Chain Attack

A *supply chain attack*, also called a value-*chain* or third-party *attack*, occurs when someone infiltrates your system through an outside partner or provider that has access to your systems and data, or provides you with tools that bad actors can compromise and use those tools to penetrate your network.

Synthetic Identity

A synthetic identity is fake identity created by a fraudster in order to take advantage of and profit off of a service that serves people. For example, fraudster creates a synthetic identity to get a bank loan or credit card issued to them.

Synthetic Media

Specialized software modules that look at the PC and make sure nothing gets changed by malware, and sometimes are able to either block changes or revert the system to its original state. See ‘Active Protection’.

System 1 Thinking

Perry Carpenter: We'll start with the work of behavioral economist Daniel Kahneman. In Kahneman's work, "Thinking Fast and Slow," he describes two types of thinking - System 1 and System 2. System 1 is very fast. It's emotion-driven. It takes shortcuts. And it's great, but taking shortcuts means that our minds are constantly making assumptions, and that can lead to errors. So System 1 is fast, but it's error-prone. And System 1 is driven by heightened emotion or just relaxing into a decision and doing what feels right at the time - what comes in the moment.

System 2 Thinking

Perry Carpenter: System 2 is much slower. It's more methodical. It takes effort, and we don't often like the mental process of putting in the effort, but it leads to better, more reliable results. Now, the problem with all of this is that System 1 accounts for about 95% of our thinking and actions, and System 2 accounts for only 5% of our thinking. Think about that - about 95% of our thoughts and actions are governed by emotion and taking shortcuts and can have the tendency to be error-prone. That's not a good ratio.

T

TTL

Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router. TTL is also used in other contexts including CDN caching and DNS caching, and we are adding another perspective here in the form of the *ever shrinking* average lifetime of

to use a service. Usually, such terms are legally binding. Terms of service can cover a range of issues, including acceptable user behavior online, a company's marketing policies, etc. Some organizations, such as Yahoo and Facebook, can change their terms of service without notice to the user base. Here is Knowbe4's TOS

TCP/IP

Transmission Control Protocol/Internet Protocol. This is the protocol that the Internet uses to transport data packets from one computer to another.

Tabnabbing

Uses browser tabs to impersonate legitimate websites and create fake login pages that trick victims into revealing private information. Tabnabbing works when you have two or more tabs open in a web browser. When a tab is left unattended for several minutes, a tabnabber can redirect the site in the unattended tab to a different, malicious login site.

Tailgating

A method used by social engineers to gain access to a building or other protected area. A tailgater waits for an authorized user to open and pass through a secure entry and then follows right behind.

TELNET

Telnet was developed in 1969 and one of the first Internet standards. The name stands for "teletype network". Telnet is a communications protocol for applications that use 2-way interactive text, using what is called a "virtual terminal" connection. Telnet runs on top of the Transmission Control Protocol (TCP).

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote computer. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The term telnet is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection with the Telnet protocol as in "To change your password, telnet to the server, log in and run the passwd command." More at WikiPedia

Tenant Separation

Test Harness

(IEEE) A software module used to invoke a module under test and, often, provide test inputs, control and monitor execution, and report test results.

Test Suite

A collection of test cases used to validate the behavior of a product. There may be several Test Suites for a particular product for example. In most cases however a Test Suite is a high level concept, grouping together possibly hundreds or even thousands of test cases related by what they are intended to test.

Token

1) In general, a *token* is an object that represents something else, such as another object (either physical or virtual), or an abstract concept. An *authentication token* securely transmits information about user identities between applications and websites. More.

2) In Natural Language Processing (NLP). Tokenization is the process of breaking down a piece of text into small units called tokens. A token may be a word, part of a word or just characters like punctuation.

Tower Dump

Many law enforcement agencies use a surveillance tactic called “tower dump.” The method gives police access to “identity, activity and location” data of users and makes use of multiple [cell phone] towers, and wireless providers, and can net information from thousands of phones. Records show that at least 25 police departments own a Stingray device – which essentially operates as a fake cell phone tower in order to siphon data from nearby phones that connect to it. This was the method that ultimately caught Kevin Mitnick.

Tradecraft

The word "tradecraft" is most often associated with spies. But hackers hackers and social engineers also have their tradecraft: a set of techniques they use to get illegal access to hardware, software, or deceive humans.

Transport Layer Security

opening a file, running a program, clicking on an e-mail file attachment).

Trojan

A Trojan horse (shortened to trojan), is non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system. The term is derived from the Trojan Horse story in Greek mythology. It is the most prevalent form of malware in the timeframe 2010-2014, well over 50% of all malware are Trojans.

Trojan downloader, also called 'Trojan dropper'

A Trojan Downloader is a program typically installed through an exploit or some other deceptive means and that facilitates the download and installation of other malware onto a victim's PC. A Trojan Downloader may download adware, spyware or other malware from multiple servers or sources on the internet. See 'Exploit'.

Typo Generator

A software tool to generate a list of typos and common misspellings, for instance for domain names. (i.e. www.goofle.com) These domain names are then used to create a perfect copy of the original, and users tricked into leaving confidential information. This is only one example of typo generator use, many more are possible.

Typosquatting

Purchasing web domains that are a character or two different from a legitimate and well-known social or company website. When a person mistypes the web address, a website appears that looks very much like the intended site. Typosquatting is usually done for fraudulent purposes. Also called URL hijacking.

U

Focuses on the automated detection of known and unknown security risks and threats that signature and rules-based security solutions cannot identify. UEBA uses behavior analytics powered by machine learning to automate data collection and generate risk-scored intelligence for each user and entity on the network.

URL shortening

A method of reducing the size and complexity of web URLs, mainly for ease of use. However, URL shortening also disguises a website's real domain name, and hinders detection of known malicious sites or destinations.

USB-Stick

A USB memory stick often used for penetration tests, with malware on it that exposes the network to the attacker. Also called Thumb-drive. The drive is left at common areas like a parking lot or the rest room, and had a label that make the user want to know more, e.g. "Q1 Layoff List".

Unit Testing

Testing of a software module for typographic, syntactic, and logical errors, for correct implementation of its design, and for satisfaction of its requirements. Also called component testing.

Update

A software 'update' is usually a patch. A patch is a piece of software designed to fix problems with a computer program or its supporting data. It can include fixing security vulnerabilities and other bugs, and improving the usability or performance.

Upgrade

The term 'upgrade' refers to the replacement of a product with a newer version of the same product. In software, it means a replacement with a newer or better version, in order to bring the system up to date or to improve it features. See (and contrast with) 'Update' above.

Usability Testing

Tests designed to evaluate the machine/user interface. Are the communication device(s) designed in a manner such that the information is displayed in an understandable fashion enabling the operator to

V

VAR

A value-added reseller (VAR) is a company that adds features or services to an existing product, then resells it (usually to end-users) as an integrated product or complete "turn-key" solution.

VB100

This stands for “Virus Bulletin 100% Pass”. It means an Antivirus product catches all the malware that is on the WildList and also has NO False Positives. Getting awarded the VB100 is important in the industry and shows a product has attained a certain quality level. It does not mean it catches 100%, no antivirus product does. Here is the Virus Bulletin website.

VDI

A Virtual Desktop Infrastructure (VDI) allows a user’s desktops and applications to run in a private virtual machine hosted on servers in a data center rather than locally on the user’s PCs. It’s technically complex and expensive, but it allows users to access their personalized desktop from any PC; and makes life easy for admins.

VEC

Vendor Email Compromise. This is a variety of business email compromise (see BEC) attack in which attackers gain access to email accounts at a company in the supply chain, and then use the accounts to target that company’s customers.

VLAN (virtual local area network)

VLAN (virtual local area network) is a way to separate or group some of your network traffic from your other network traffic. You would set this up to improve network security, performance, and provide easier management.

VPN

Virtual Private Network. VPN vocabulary: all the key terms and jargon explained

Virtual Machine (VM)

A computer resource that runs programs inside a software created “virtual” operating environment rather than on a physical computer. Each virtual machine runs as a separate computing environment, allowing different operating systems to function simultaneously on the same “host” machine. VMs can even be used on the cloud to provide virtual application resources.

Virus, also called ‘File Infector’, or ‘File Virus’

A computer virus is a computer program that can copy itself and infect a computer. The term “virus” is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. Since 2009, viruses in their traditional form are less than 10% of total malware. Microsoft in 2010 estimated it was only 4%. A true virus can only spread from one computer to another (in some form of executable code) when its host (infected file) is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it (via sneakernet) on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system. See ‘Worm’. See Wikipedia.

Virus Bulletin

Virus Bulletin is the world’s first and foremost virus and malware authority, and the go-to place for the antivirus industry.

They do three things: 1) a monthly magazine, 2) an annual conference and 3) bimonthly product certifications.

1) Their name comes from the first thing they started with in 1989: **a magazine** dedicated to providing PC users with a regular source of intelligence about computer malware, its prevention, detection and removal, and how to recover programs and data following an attack. Virus Bulletin quickly became the leading specialist publication in the field of malware and spam and is today produced in an online format.

2) **VB Conference**. They first VB conference was in 1991 and the event has become a major highlight of the anti-malware calendar. They present factual information, demonstrate defensive procedures and countermeasures, and provide a platform for experts share their research and set new standards.

3) **“VB100″ certification**
For many years, Virus Bulletin has carried out independent comparative testing of anti-malware products. The unique VB100 certification is widely recognized within the industry. Virus Bulletin tests anti-malware

the VB100 is important in the AV industry and shows a product has attained a certain quality level. It does not mean it catches 100%, no antivirus product does.

Virus Definitions, abbreviated to 'Defs', also called 'Patterns' or 'Signatures'

The database of virus signatures (detections, patterns) that allows an antivirus product to recognize and disinfect viruses. These definitions are created by an AV Lab team and send to PC's running that Antivirus very regularly.

Virustotal

Virustotal is a website that delivers a service which analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by about 70 different antivirus companies that scan the file so you basically get the opinion of many different security companies at once. Both good guys and bad guys use Virustotal. The bad guys send their malware up there to see if it gets caught by antivirus engines. It's got free and paid license versions and is owned by Google. You can find them here.

Vishing

A phishing attack conducted by telephone, usually targeting voice over IP (VoIP) users, such as Skype users. Vishing is the phone equivalent of a phishing attack. There are two forms of this, human and automated. In the human example a scam artist uses the anonymity of a phone call and pretends to be a representative of their target's bank or credit card company. They manipulate the victim to enter their PIN, credit card number, or bank account (and routing number) with the phone keypad. This allows the scammer to get instant access to another person's bank credentials.

It's also known as rogue "IVR" (Interactive Voice Response) and that is where it gets automated. The bad guys use an IVR system to impersonate a real-sounding financial institution's IVR system. Using a phishing email, the victim is told to call "the bank" using their toll free number, so that the fake bank can "verify" some information. A normal trick is that the system is configured to throw fake error messages so that the victim will try several passwords to get in. More sophisticated scams even have a live body impersonating customer service in case the victim presses "0" for an operator.

Vulnerability Management

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing, and remediating software vulnerabilities.

Voicemail overloading

Spamming over Internet telephony. Much like getting spam email, a voice over Internet Protocol (VoIP) user can get junk voicemails. Spammers simply send a voicemail messages to thousands of IP addresses at a time.

W

WYSIWYG

What **Y**ou **S**ee **I**s **W**hat **Y**ou **G**et - A term in the computer world that means you are working in an environment that is visual. As an example, when you edit something in a WYSIWYG editor, you literally see the changes and how they look, (for example a word processor) as opposed to an HTML editor where you work in code, and you need to render the code into a webpage to *see* the changes you made in the code.

Wake-on-LAN

A Wake-on-LAN (WoL) is a networking standard that allows a computer to be turned on or awakened by a network message. That message is usually sent to the target computer by a program executed on a device connected to the same local area network, could even be an admin's smartphone. This technology can also be used in Wide Area Networks, and even Wi-Fi, a standard called Wake on Wireless LAN (WoWLAN) More about this at Wikipedia.

War Dialing

A technique by which a computer will dial a number repeatedly in a telephone exchange in an attempt to circumvent perimeter security.

Web, How it Works

large scale. Enter **Web 2.0**, which was a 'read-write' architecture with user-generated content, a participatory culture and interoperability. To make Web 2.0 really work, you needed centralized infrastructure, data and services. The companies that provided those things became the winners, creating valuable network effects. But the ever growing success has led to questions around the degree of centralization – and whether users themselves have become the product. (Remember, if it's free, *you* are the product.)

Next: **Web3**, a decentralized but secure internet. In its purest form, Web3 is 'trustless' (networks allow participants to interact without going through a trusted intermediary) and 'permissionless' (anyone can participate without authorization from a governing body), running on blockchain technology and incentivizing engagement via tokens (which really are verified ownership stakes). *Tip 'o the hat to Dan Dees & Jim Esposito @ GS.* Here is a great background article at CBINSIGHTS. And here is a glossary that contains most of the important web3 jargon that you need to know.

Web Filtering

Stand-alone software or an appliance (hardware+software) that blocks access to specific Internet websites. A survey done by KnowBe4 shows that system administrators want web filtering on their network for the following reasons:

- Block access to malware sites
- Block access to inappropriate or damaging sites
- Keep users "on task" meaning productivity
- Adding another layer of defense second to AV
- Reduce network bandwidth
- Keeping HR happy

Website Log

A log is a running record of everything that is constantly happening on a website or in a system. It contains various data points e.g., timestamps with user actions like, "John Smith clicked on the training tab at 09:00 AM EST". Website Log files can help analysts identify slow response times of webpages, errors, bugs that impact the website, and defend against attacks on the website.

Westcoast Labs

A commercial organization that tests AV products to see if those products catch all the samples in the WildList. If a product gets all the samples, a certification gets awarded. Here is their website.

The list of known good files that Antivirus knows do not have to be scanned and should not be quarantined. Can also apply to domain names, which are known to be good and allowed access to. Also, a list of known-good executable files that are allowed to continue to run in an environment that has Application Control enabled.

WildList (also abbreviated as WL)

A varying list of around 800 malware samples that are 'in the wild', put together by the Virus Bulletin WildList committee. AV products are expected to catch all samples that are in the WildList.

Windows System Files

System Files are the files that make up the Operating System. These files are protected from deletion or infection by System File Protection (WFP) in Windows 2000, renamed to Windows File Protection (WFP) in Windows XP, and then to Windows Resource Protection (WRP) in Vista and later. WRP introduces protection of the registry.

Windows Update

A free service from Microsoft that regularly updates your PC with the latest bugfixes and security patches and then reboots the PC. For consumers it is highly recommendable to have this set on automatic. Microsoft does this on the second Tuesday of the month, called Patch Tuesday. Businesses should use their own centralized update server, after they test the patches in their environment for compatibility issues.

Workstream (security workstream)

OK, We are going from *generic* to *specific* here for this definition. First, a workstream (also known as workflow) is *a core area of an activity or project*. It's a core process, it can be big and it can be small, depending on where you look. Here is an example to make this a bit more real. If you are planning for a wedding, that's a project. It has a start and end date, it would involve multiple stakeholders and many workstreams. An important one is selecting a caterer. In this instance the *workstream* would be named 'Catering' which is the core process. The activities within this workstream would be the following:

- Meet with caterer
- Plan 5 course meal
- First tasting session
- Second tasting session
- Finalize Menu

process of an employee seeing a phishing email, clicking the **PAB,** this being received in PhishER, looked at by an analyst, and then processed is a **great example of a security workstream**. If an organization does not have this security workstream, they should!

Worm

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing file. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Worms can spread with lightning speed. One worm was able to infect hundreds of thousands of servers worldwide in less than 10 minutes.

X

XDR

Extended Detection and Response (also see EDR) XDR is a newish approach to threat detection and response that Gartner called a top security and risk management trend of 2020. It combines elements of **S**ecurity **I**nformation and **E**vent **M**anagement (**SIEM**), **S**ecurity **O**rchestration, **Automation**, and **R**esponse (**SOAR**), **E**ndpoint **D**etection and **R**esponse (**EDR**), and **N**etwork **T**raffic **A**nalysis (**NTA**) in a software-as-a-service (SaaS) platform to centralize security data and incident response. This improves and speeds up detection of and response to bad actors in your network because it correlates threat intelligence across security products and visibility across networks, clouds, and endpoints. (Read this article for more)

something, and very often used to analyze possibly malicious email messages. Those rules are conveniently called YARA rules.

Z

ZBB

Zero Bug Bounce. A milestone in software development when all the known bugs are fixed and the bug count drops to zero. Usually, the next day a few more bugs are found, so the bug count “bounces” up from zero. Indicator the product is nearly ready to ship.

Zero-day Attack or Zero-day Threat

A zero-day attack is a computer threat that tries to exploit vulnerabilities that are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Bad guys have a field day with zero-day attacks, as there is very little defense against these. There are many of these vulnerabilities for each software product, and there is a lively trade in zero-day vulnerabilities. Both governments spy agencies and cybercrime buy these exploits often for tens of thousands of dollars.

Zero-day Exploits

Actual code that can use a security hole to carry out an attack. Used or shared by attackers before the software vendor knows about the vulnerability.

Zero-hour phishing threat

A zero-hour phishing threat—very similar to a zero-day threat—is a phishing attack that hasn't been seen before and doesn't match any known signatures. This makes it very hard to detect by traditional signature-matching solutions

Zero Trust Network Technologies

perimeter. Instead, the zero trust model stresses that everything and everyone attempting to connect to systems must be verified before granting access. In a zero trust environment, organizations are able to monitor the entire IT environment for signs of malicious activity.

Zombie, also called 'drone'

A PC that has been taken over by malware and is 'owned' by the bad guys. The PC is now part of a botnet and spews out spam, tries to infect other computers, attacks websites or does other nefarious things. Government spy agencies like the NSA also use this tactic and have tens of thousands of machines infected and basically own them.

- Integrations
- KnowBe4 Ventures
- KnowBe4 Blog
- Careers At KnowBe4
- Patents
- Federal

Free Tools

- Phishing Security Test
- QR Code Phishing Security Test
- Phishing Reply Test
- Social Media Phishing Test
- Multi-Factor Authentication Security Assessment
- Domain Doppelgänger
- Awareness Program Builder
- Password Exposure Test
- Phish Alert Button
- Email Exposure Check Pro

- Domain Spoof Test
- Browser Password Inspector
- Mailserver Security Assessment
- Ransomware Simulator
- Second Chance
- USB Security Test
- Breached Password Test
- Weak Password Test
- Training Preview
- SecurityCoach Preview

Phone: 855-815-9494

Email: support@knowbe4.com

Search

Search