wizer
wizer-training.com

Wizernary - Translating Geek to English

Have you ever nodded your head to pretend to know what your Tech Team is talking about? Now you don't have to! Enjoy a fabulous collection of technical definitions with all of the wit, humor, and sarcasm of Wizer Warlock, Chris Roberts!

#

2FA (Two-Factor Authentication)

A

Admin Privilege
Adversary
Advanced Persistent Threat
Artificial Intelligence (AI)
Attack Vector
Authentication

B

Blockchain
Botnet
Breach
Brute-force
Bug
BYOD

C

Cloud
Cookie
Cyber
Cyber Security

D

Denial of Service (DoS)
Distributed Denial of Service (DDoS)
Digital Transformation
Domain

E

Encryption
Exploit

F

Firewall
Firmware

G

Ghosted

H

Hacker
Health Insurance Portability and Accountability Act (HIPAA)

https://web.wizer-training.com/translating-geek-to-english

J

Comong Soon

I

Identity Theft
Incident Response Plan
Information Technology
Internet of Things (IoT)

K

Keylogger

L

Leet Speak (1337)
Long lost Uncle

M

Media Access Control (MAC) Address
Machine Learning (ML)
Millions in the bank

N

Nigerian Prince

O

Coming Soon

P

Penetration Testing (Nice Version)
Penetration Testing (The Rant)
Ports

R

Ransomware

S

Scam
Spoofed
Spyware
Steganography

T

Text Code
Trojan

V

Coming Soon

W

Wetware
Won the lottery

Z

Coming Soon

#

2FA (Two-Factor Authentication)

Two things to work out you are who you say you are... Typically, one is a password and the other is either your email, your phone, or something “about” you. (face, fingerprints, eye, etc.)

That code you get on the internet

A

Admin Privilege

Power corrupts, absolute power corrupts absolutely… it’s like having the master key to life, but in the digital realm.
When your phone or system lets you make whatever changes you want, irrespective of any consequences beyond simply asking “are you sure?”

No permission required...

Adversary

Our digital enemy, they’re out there, in the trenches, the forest, or the building next door, just watching for that opportune moment to take advantage of you, your family, team, company, or the supply chain you so perilously rely upon.

Someone who wants to steal from you or do harm to you

Advanced Persistent Threat

It's like the digital version of WMDs. We'll scream from the top of our lungs that we're about to be brought to our knees with APTs coming in from (pick a country we don't like at the moment) until someone gives us money OR allows us to go on the rampage. Then we find out we actually got breached because some numpty left the digital keys under the front door mat.

Really sneaky adversary who doesn't set off the alarms

Artificial Intelligence (AI)

Think Clippy from Microsoft but slightly smarter. We like to think it's better, but in reality, in most vendors cases…it isn't.

No permission required...

Attack Vector

It's the digital equivalent of you leaving your door open, or your window ajar, or car unlocked. It's simply another way to say how someone may attack you or take advantage of you. It's simply the method used to break into you.
How do I love thee? Let me count the ways… See, even Elizabeth Barrett Browning was doing assessments in the 1800's.

Taking advantage of you

Authentication

This is simply the name for the process by which we work out - "you are who you say you are". Be you're at the ATM and having to put your PIN number in, or sitting at a keyboard typing in a password, or looking at the phone while it decides if that moustache is real or false…they are all methods of authentication. It's simply working out if you are true, genuine, and valid.

Remember trust AND verify… this is the verify part.

B

Blockchain

Remember the old way of doing accounting? Two ledgers, it's a digital version of that, but a whole lot more ledgers and a LOT more accountants, all working furiously to record transactions and make sure that they agree AND that nobody can mess with the books.

It's a digital version of your check register that's shared with ALL your friends and family

Botnet

Your computer...really, it's YOUR computer, or anyone's system that's infected with malicious code, that's then used to attack and infect others.

A lot of computers being controlled by someone else other than their owners

Breach

Remember the Dutch story about the kid that saved the country from flooding? Yea, it's like that, but there's no kid, the hole's big enough to drive a bus through, and the water? That's YOUR data leaving…
Someone you didn't invite in just backed up ALL your data, snuck it out, and has it.

When someone breaks into your home, office or computer

Brute-force

When I don't know the answer, I guess… and the system lets me keep guessing. Mostly used against passwords where I can "guess" up to a billion times a second using certain types of computer equipment.

Using a digital sledgehammer to crack the walnut

Bug

In computer terms (and not Mother nature's creepy crawlies), it's a coding error, a flaw, an error, or someone, somewhere forgot to put a "; " where it was needed… the program will often still work, but somewhere, something has taken notice and it's eating memory (making your computer slow) or simply it'll stop working (for those of you old enough the Microsoft blue screen of death…)
It's estimated that there's 15-50 "bugs" per 1,000 lines of code, and most modern cars have 100 million lines of code in them… think about that next time you are speeding on the motorway.

It's a flaw, unless you are Apple or Microsoft in which case it's an enhancement.

BYOD

Bring Your Own Device...What it really means is that the company doesn't want to buy you a computer or phone and you can use your own OR they want to give you one from the stone age and yours is better…

Using your personal device to do work on...

Cloud

The easy answer is "it's someone else's computer," BUT that like comparing an AMC Pacer to a Bugatti Chi ron… Technically true, but about as far from the reality of things as possible. Think of cloud computing as VERY specifically designed and built for one core purpose…the flexibility to allow the rest of us to move all our data, systems, and lives TO it with minimal fuss and hassle…
Next doors computer (you know I had to leave that one in…)

Shared computers and storage in large buildings all over the world

Cookie

It's not edible, at least by you… your computer likes them and websites LOVE feeding them TO your computer. Some of them are nice, the good ones just want to remember what you looked at, what your preferences are, and they help with customizing your experience ON the website. However, there's a LOT of cookies out there that are NOT nice and are used by advertisers NOT associated with the website you are on. Typically, they are called 3rd party cookies and they will track you, your movement, and do their level best to profile you and work out how to sell you something or worse.
Think of them as a digital fingerprint of where you've been on the Internet, what you looked at, and what you did…

It's a digital (software) tracking device.

Cyber

This is one example of where marketing won over common sense. Cyber is simply the collective name that's been associated with anything related to the Internet, computers, and the digital age. It's a combination word taken by blending computers, networks, virtual reality, visions of the future, and whatever else they could find to make Information Technology sound cool and appealing.
We can go back to the Greek and take their word for pilot or steersman (nautical) as those who held the future, and we've also got the 1940's to blame with cybernetics which was the study of control systems and the communications between people and machines. Ultimately though, Information Technology was too much of a mouthful, so cyber was resurrected, dusted off, and the marketing machine ate it up.

Technology… OR a box of microchips doing something fancy…

Cyber Security

The protection of computers, networks, systems, hardware, software, and all things related. To protect from theft, damage, or attack by others. To guard against disruption, misdirection, and to safeguard the data entrusted to us. That's meant to be the heart of Cyber Security. Arguably, we have one job, to protect others. People before process and always before technology.
To ensure confidentiality, integrity, availability of information, and the very systems we all rely upon.

The digital guardians

Denial of Service (DoS)

Think of this as someone unplugging the Internet, or part of it… you can't get to what you want, your web browser's sulking, and Netflix is offline. IF you are experiencing a DoS then it means you've annoyed someone enough that they worked out how to unplug you or your computers from the Internet, either by attacking your network devices or computers. (office ones or on the Internet somewhere)

Stopping you from using your digital world

Distributed Denial of Service (DDoS)

Like the Denial of Service but typically done from a whole lot of different computers…think of this as the movie "300." You're guarding that passageway and a WHOLE LOT of digital Persians are throwing the entire digital version of the kitchen sink at you…eventually you're going to fail…so go make a cuppa tea and start to go through your Incident Response Plan. (see below)
Remember those times at a party or when you're out enjoying yourself, there's a crowd of noise and you're trying to hear ONE person, OR when everyone's talking to you at the same time and you're trying to listen to ONE voice… that's a distributed denial of service.

Think of this as the digital version of turning it up to 11…

Digital Transformation

The use of digital technology to supplement people and processes in solving problems. Taking something that was manual or human intensive and working out IF and HOW technology could help. The greater goal of digital transformation is cultural and breaking down borders and barriers by bringing everyone together to solve problems, share solutions, and simply benefit humanity in all manner of unique ways.
By bringing a diverse cultural experience to a wider audience. In simple terms, it would be a market trader in Uganda figuring they could sell their goods online. (Etsy, Amazon, Etc.) All of a sudden, they've got an audience of 4 billion as opposed to whoever's passing by on the street. It's got benefits (audience) and challenges! (shipping, logistics, tracking, etc.)

Opening a business's eyes to the digital world…

Domain

An Englishman's digital castle… Think of a domain as your piece of the digital world. You've decided to go onto the Internet and want to stake your claim. (remind anyone of the Oregon Trail game… same idea, and as bad a consequence sometimes). A domain is yours (rented for however many years you pay) where you can put whatever you want in it or on it. Congratulations, you can become the next Amazon, OR could fade away like Myspace…

It's your own country in the digital world.
It's that first part of that address you type into the browser…
(Amazon, Yahoo, Facebook, etc.)

Encryption

Think of this as the digital version of the WWI and WW2 Windtalkers (or code talkers) that were engaged by the US Military. Originally, the Cherokee and Choctaw peoples helped in the first Great War, then the Navajo in the second. The logic being that only the sender and recipient can understand the message, and to everyone else it's simply noise.
Turning perfectly usable data into mumbo jumbo since 1900BC, or around 1990 if we are talking the modern digital equivalent.

It's the digital version of invisible ink.

Exploit

In the physical world it's the crowbar that was used on pandora's box, or the same one used to get into your house, shed, or car. It's simply the act of taking advantage of a vulnerability OR causing a situation where a vulnerability opens up...

To take advantage of you.

F

Firewall

It's meant to be a barrier between you and the rest of the Internet when you are sitting at home or in your office, it's meant to protect you from some of the bad stuff out ON the Internet (or the office next door), but in practice it's as leaky as an old sieve and as much use as a chocolate fireguard. The problem is, it can't BE a barrier because it has to let SOME traffic through (the stuff you WANT to see) but in opening that door it's not very good at stopping uninvited guests from sneaking in too. It tries to ask everyone for their invites, or to ask them why they want to come in, but the attackers are sneaky and will lie to your firewall, and unfortunately, most of the time, it believes the lies.
It's like Jeeves at home, it's great at being nice to the right guests who come to the front door, and it can sometimes catch the ruffians trying to sneak in, but it's fairly useless at watching the windows, the back door, and heavens forbid someone sneaks in through the coal chute... You can't pension Jeeves off, but you can't rely upon him to REALLY guard the place.

The digital butler, great if you abide by the rules, totally flummoxed otherwise

Firmware

It's the programs that make the hardware work. When you mash a key on the keyboard OR you yell at Alexa OR print something there's a layer between what you've done and the app or computer software that shows you the results. That's the firmware. The keyboard tells the firmware what was pressed, that then tells another piece of software in the operating system (Windows, Linux, Mac, iOS, Android) what you did, and then lo and behold it appears on the screen in the right place… Same for Alexa, the sound hits the microphone which translates waves into 1's and 0's, the firmware tells the software what it heard and the rest happens…it's the layer that makes things work.

To take advantage of you

Ghosted

As in the physical world, so be it in the digital one… In the human world, ghosting means to abruptly end a relationship by burning the cards, throwing away the phone, and deleting the email account… in the digital realm, it's when that's done TO you… All of a sudden you don't exist, your cards don't work, you have no credit, and apparently your social security/national insurance number was given to a squirrel that's now stuffed on the mantlepiece of your adversary. You have become a non-entity, congratulations now you can join the CIA ;-)

You've been erased, wiped out, digitally you are no more.

H

Hacker

That'd be me, us, a community and a LOT of folks who are day-walkers OR who don't necessarily prance round in hoodies ALL the time. We're the good folks, and according to Hollywood, we can stop ships, take control of power stations, AND hack aliens using an Apple Mac. Apparently, the media and the marketing folks in our industry didn't get those particular memo's.

We're the tinkerers, wizards, witches, and warlocks of the digital age…

I

Identity Theft

Why be you when you can be new? OR why be you when you can be someone else? Identity theft is simply the act of becoming someone else for the sake of financial gain, enforcement, avoidance, or something else where being "you" is detrimental to the situation. In the real world, as kids, some of us would forge our parent/guardian's signature on the homework record. In the digital world, it would simply be the act of becoming the parent…

In the digital world we truly can be anyone we want to be…

Incident Response Plan

When all hell is breaking around you, and you're sitting in the middle of things as calm and as cool as a cucumber. It's because YOU have a plan. You know what to do, where to be... and as soon as you can get everyone's attention, you'll start to bring order to chaos. Think of the IR plan as a series of instructions on what to do just before the end of the world.
It's our version of those flight safety cards. Instead of telling you to put your head between your legs and kiss your ass goodbye, we simply want you to unplug the computers, grab the office dog, and exit safely.

A set of Instructions for when all hell breaks loose

Information Technology

It is the application or use of technology to store, retrieve, transmit, and work with data. (information) It' s typically applied within the business world, but has its modern origins firmly rooted in the mid 1940's when the first programmable digital electric computer was designed and used (Colossus) for deciphering enemy encryption. Since then, information technology has infiltrated almost every facet of modern life as we strive to store more, read more, and share more, faster and faster with each passing year.

The origins of our digital world...

Internet of Things (IoT)

This has become the collective noun for everything that has a microchip in it that's connected to a network. From the toothbrush that talks to your phone, to the fridge and microwave arguing with the doorbell… It is the billions of devices we are surrounded with that are apparently meant to make our lives easier and free up time. From your home, your vehicle, place of business, and everything in between, we interconnect these devices in the hopes they help us.

It's Skynet before gaining consciousness

Internet Protocol (IP) Address

If you look at an IP address, it's often 4 sets of numbers separated by a "." Each block has a meaning and each part of that block will help speed your digital message, mail, or YouTube video to and from the right place. (Most of the time… Like the post office, sometimes it DOES go pear shaped.) We have two different types of addresses, but for all intense and purposes, they do the same thing…they help work out where to send your digital life.

Your digital street address on the Internet

K

Keylogger

These are programs that watch what you type. They sandwich themselves in the digital world between your keyboard and the operating system or on a mobile device. They often hide RIGHT in front of you as a “cover” for your keyboard (it looks just like your normal keyboard on your phone.) Their job is to simply record everything you type (mistakes and all) on the keyboard. They are logging passwords, messages, notes, where you go on the Internet, or who you’re talking with. That data is then sent to whomever installed the program on your machine. Often times, they do this without you knowing about it. They’re sneaky, malicious, and often go undetected for a long time.
Remember the Yellow Pages advert “Let your fingers do the walking?” A keylogging program would be the one watching those fingers walk… EVERYWHERE…

It’s the unwanted digital assistant watching your every move.

L

Leet Speak (1337)

These days, more often than not, it’s someone who drank too much of their own Kool-Aid, or hasn’t found their way out of the bulletin boards. (Our digital meetings places before we had Myspace, Facebook, Etc.)
It’s a form of substitution using characters, numbers, and other things to substitute the alphabet within a word. (Hacker becomes h4x0r, etc.)

1t's 4ll gr33k t0 m3 (It’s all Greek to me…)

Long Lost Uncle

See Scam .
Your uncle never was lost in the jungle, nor did he leave a fortune in the bank, nor does that person at the other end of the email OR phone call REALLY care about you. Hang up and never answer the message. Please.

Media Access Control (MAC) Address

A unique code given to every single network interface controller ever made. This is the physical part of the puzzle that allows systems to find and talk with each other in the digital world.

Your physical street address on the Internet

Machine Learning (ML)

See Artificial Intelligence. Just slightly dumber than Clippy.

Millions in the Bank

See Scam.
Even if I do have cancer...or I'm terminally ill, I'm not leaving my fortune to you, a total stranger whom I've just met on the Internet. Seriously, if I have millions in the bank, the relatives will be crowding round me like a pack of vultures and you, my Internet friend, will see nothing but an IOU. So run and run, now and never answer that email. Please.

N

Nigerian Prince

See Scam.
Nigeria is a republic, ruled by a democratically elected president, so no prince here.
Nigeria is also a federation of 36 states, so no central prince, however there ARE parts of the country that still maintain a tribal or ethnic view that a person can be chosen to represent their community or town, however their jurisdiction is limited, and the chances of them having a few million in the bank JUST to send to you is so far from reality we've not even discovered the science to find it. So, don't respond, ever. Please.

P

Penetration Testing (Nice Version)

Think of it as the digital equivalent of a friendly break in, where the burglar leaves helpful notes ALL over the house. Reminding you to lock your doors, to turn on the cameras, not to leave the keys for the cars on the shelf, and that you should really change the combination to the safe. You get all the lessons, you have all the information at your fingertips to help you improve, make changes, AND you have the logic as to "why" to do this. Testing and assessing done in collaborative settings can help all parties learn about themselves in a manner that's controlled, safe, and educational.

Realism without the lawyers and headaches

Penetration Testing (The Rant)

If approached incorrectly, it can be an outdated and outmoded method of shaming a company into paying more money for binky shit that they don't need. IF done right (and there's only a few places that are good) it can be a collaborative, cooperative experience where both parties benefit.
Penetration testing puppy mill, a company that employs cheap bodies, gives them crappy tools and then rebrands Nessus reports as "assessments" and charges for the pleasure. (See Scams.)
Even within our own industry, we can't agree what a penetration test is or what a scan or an assessment is... Therefore, I'm not even going to attempt to do it. Suffice to say, when someone wants to "test" you, make sure you know what you're getting into, what questions to ask, and expectations to have, AND make sure it's a reputable company that WILL take the time to educate you, help you improve, and isn't in it for just the money.

You're naked, and they have 50 gallons of lube and rubber gloves

Ports

Windows and Doors

Ransomware

Evicted and Locked Out

S

Scam

The world of fraud and the tricksters themselves have found the Internet and with it, they can scheme and scam tens, hundreds, and thousands of people at once. Where before they were the street hustler, peddler, or petty criminal; they can now, with the aid of a computer and some simple programs, trick targeted groups of people in ever increasingly innovative ways.
There is no pot of gold at the end of the rainbow, the cake is a lie, the check is not in the post, you are NOT a winner, and no, you're not getting your long-lost uncle's inheritance from outer Mongolia IF you just pay a little something up front.

1001 digital ways to part you from your money

Social Engineering Attack

Fraud, Scam, Duped

Spoofed

Faked

Spyware

Virus Software

Steganography

Picture, video, or music file with hidden messages- some deemed malicious

T

Text Code

See Two -Factor Authentication. Typically, the way to check you are who you say are is by the company or website (bank, Amazon, etc.) sending a code to the phone THEY think you have (or you told them that you own).

Trojan (or Trojan Horse)

Hidden Virus

W

Wetware

You, the user.

Won the Lottery

See Scam.
No, you didn't win, neither did you come in second, or get another bit of the apple, and even (by some fluke) you DID win, do you really think they'd ask you to either prove who you are OR ask you to pay THEM money for the money they owe you? No. Never. It's NOT how it works. So, don't hand over your identity, your money EVER. Please.

Resources for Inspiration

https://learn.g2.com/cyber-security-terms
(https://www.linkedin.com/in/mara-calvello/)
https://www.linkedin.com/posts/gabrielfriedlander_informationsecurity-cybersecurity-securityawareness-activity-6681556963135909888-j4Z
https://blog.securityshitshow.com/2020/06/shit-show-episode-7.html