

Unit 5: Impact of Computing

Unit 5 asks what computing does to people, not how programs work. It covers computing innovations and their beneficial and harmful effects, the digital divide, bias in computing, crowdsourcing, legal and ethical concerns including intellectual property and Creative Commons, and safe computing practices for protecting your data.

AP Computer Science Principles

Impact of Computing

About 15 minutes to read

How to use this guide

Read it in order the first time because the unit builds from ideas to consequences. Start with what counts as a computing innovation and how to describe its effects, then move to who has access to technology, how data and bias shape outcomes, what the law allows, and how to protect yourself. Exam questions are almost always scenarios, so as you read, practice naming the exact term each situation illustrates.

After the first read, use the trap boxes and the Confusions table to review the distinctions the exam tests most often. Finish with the practice questions, then complete the recall check on the last page out loud and note any items you cannot explain yet.

What this unit is worth. Impact of Computing is 21 to 26 percent of the AP Computer Science Principles exam, one of the largest shares of any unit. The questions are scenario based. You read a situation and identify the effect, the ethical concern, or the correct practice. Learn the exact definitions, because the wrong answers are built from terms that sound similar.

5.1 Beneficial and Harmful Effects

A **computing innovation** is an advance in computing that changes how people live, work, or interact. It always includes a program as an integral part of how it works. It can be a physical device such as a self-driving car or a fitness tracker, a piece of software such as a photo editor or a ride-sharing app, or a computing concept put into practice such as online shopping or streaming video.

Every innovation can be described by its **purpose** and its **function**, and the two are not the same. The purpose is the reason it was built. The function is what it actually does. The purpose of a fitness tracker might be to help people exercise more. Its function is to record movement, heart rate, and sleep using sensors and software. When a question asks you to describe an innovation, state both.

Computing innovations are usually designed for a specific purpose, but they produce effects the designer did not plan. Effects can be beneficial or harmful, and the same innovation can be both at once. A ride-sharing app makes transportation more convenient, which is beneficial, and adds traffic and emissions in busy areas, which is harmful. Judge effects in the three areas the exam names: **society**, **economy**, and **culture**. A social media platform changes how society communicates, creates jobs in advertising and content moderation, and spreads trends and languages across borders.

Intended effects are the ones the designer planned. **Unintended effects** are everything else, good or bad. Responsible design means considering possible unintended effects before release. When a question asks for an unintended effect, look for the consequence nobody built the product to produce.

Trap. An innovation can enable a change without causing it. Social media enabled friends to organize a protest in hours, but it did not cause their desire to protest. Exam questions test this distinction directly. If a question asks what the innovation caused, the answer must be something the innovation itself brought about, not something it merely made easier or happened alongside.

5.2 Digital Divide

The **digital divide** is the gap between people who have access to computing innovations and people who do not. Access means more than owning a device. It includes a reliable internet connection, the skills to use technology, and technology designed for your needs.

The divide runs along three dimensions the exam names. **Socioeconomic:** lower-income households are less likely to afford devices or monthly service. **Geographic:** rural and remote areas often lack broadband infrastructure, so even families who can pay have no service to buy. **Demographic:** older adults, people with less formal education, and some racial and ethnic groups have lower rates of access and use. One person can sit on several of these at once.

The divide matters because computing innovations now control access to school, work, and civic life. A student without home internet cannot complete online assignments or join video classes. A job seeker without access cannot apply to jobs posted only online. An access gap becomes an opportunity gap.

Efforts to close the divide target each dimension. Infrastructure projects extend broadband to rural areas. Subsidy programs lower the cost of service and devices for low-income households. Digital literacy programs teach skills to people who own devices but cannot use them fully. Libraries and schools provide public access points. When a question asks which effort fits a situation, match the effort to the dimension that is actually blocking access.

Trap. The digital divide is not only about money. A rural family that can afford internet service but lives where no provider built lines faces a geographic barrier, not a socioeconomic one. Read the scenario and name the dimension before you pick an answer.

5.3 Computing Bias

Computing bias happens when a computing system produces unfair outcomes for some group of people. The most common source is the **training data**. Machine learning models learn patterns from the data they are trained on, so if that data reflects past unfairness or underrepresents a group, the model learns the unfairness too.

The pattern to recognize is biased data in, biased decisions out. A hiring tool trained on a company's past hires favors the groups the company used to hire. A facial recognition system trained mostly on light-skinned faces identifies dark-skinned faces less accurately. A lending model trained on historical loan approvals can reproduce the discrimination of earlier decades. The algorithm did not invent the bias. It automated it.

Trap. Bias questions point at the data, not at anyone's intent. If a model treats groups differently, the first suspect is unrepresentative or historically biased training data. An answer that blames a programmer's personal prejudice misses how bias usually enters a system.

5.4 Crowdsourcing

Crowdsourcing enlists a large group of people, usually volunteers online, to gather data or solve a problem that would be slow or expensive for one team. **Citizen science** is the research version of this idea: volunteers classify galaxy images, count birds, or donate idle computer time to fold proteins. The shared idea is that many small contributions add up to something no individual could produce alone.

The benefit is scale. Thousands of volunteers can label millions of images in weeks. The limits are quality and bias. Volunteers vary in skill, so results need checking, and contributors are self-selected, so the sample may not represent everyone. Crowdsourced data can be valuable, but only when someone validates it.

5.5 Intellectual Property and Creative Commons

Intellectual property is the set of legal rights that protect creations of the mind. Material created on a computer is the intellectual property of its creator or the creator's organization. The ease of copying and sharing digital work is exactly why these protections exist.

PROTECTION	WHAT IT COVERS	EXAMPLE
Copyright	Original creative works such as writing, music, images, and software.	A song, a photograph, or the code of an app.
Patent	Inventions and processes that are new and useful.	A new data compression method or a hardware design.
Trademark	Names, logos, and slogans that identify the source of a product.	A company logo or a brand name.

Creative Commons is a public copyright license that a creator applies voluntarily. It keeps the copyright but grants the public permission in advance to share, use, and build on the work under stated conditions. It is how a creator says you may use this work without answering every request individually. The six licenses are built from four conditions.

LICENSE	WHAT IT ALLOWS
CC BY	Use and adapt, even commercially, with attribution.
CC BY-SA	Use and adapt, even commercially, with attribution. Adaptations must carry the same license.
CC BY-NC	Use and adapt for noncommercial purposes only, with attribution.
CC BY-NC-SA	Use and adapt for noncommercial purposes only, with attribution. Adaptations must carry the same license.
CC BY-ND	Share unchanged copies, even commercially, with attribution. No adaptations.
CC BY-NC-ND	Share unchanged copies for noncommercial purposes only, with attribution. No adaptations.

Attribution is the one condition you can never skip. Every Creative Commons license requires crediting the creator, naming the work, and stating the license. CC0 is separate from the six licenses. It is a public domain dedication in which the creator waives all rights, so no attribution is legally required.

Trap. Creative Commons does not mean no restrictions. A CC BY-NC photo cannot appear in a video that earns ad revenue, and a CC BY-ND article cannot be edited. Read the letters: NC blocks commercial use, ND blocks adaptations, and SA spreads the license to your adaptation.

5.5 Open Source, Plagiarism, and Fair Use

Open source software is made freely available. Anyone may view the code, and the license permits redistributing and modifying it. **Proprietary** software is owned by a company or person and distributed with restrictions, such as no copying or no viewing the source. The difference is the license terms, not the price. Some open source software is sold, and some proprietary software costs nothing.

Trap. Open source is not public domain. Open source code is still copyrighted, and its license sets conditions you must follow, such as keeping the license notice or sharing your modifications under the same terms. Public domain means no copyright at all, so there are no conditions to follow.

Plagiarism is using material created by someone else without permission and presenting it as your own. It can have legal consequences, and you should always cite material you did not create. Citation fixes the honesty problem. It does not fix the legal problem. Citing a source does not give you the right to copy it.

Fair use is the legal rule that allows limited use of copyrighted material without permission for purposes such as criticism, comment, news reporting, teaching, scholarship, or research. Courts weigh four factors: the purpose and character of the use, where nonprofit educational use is favored; the nature of the copyrighted work; the amount used relative to the whole work; and the effect of the use on the market for the original. No single factor decides a case, and no fixed percentage of a work is automatically safe.

Trap. Plagiarism and copyright infringement are different violations. Plagiarism is an ethical violation, presenting someone else's work as your own. Infringement is a legal violation, using copyrighted work without permission. You can commit one without the other. Citing a source avoids plagiarism but does not by itself make the use fair.

5.6 How Your Data Is Collected and Used

Personally identifiable information, or PII, is any data that can identify a specific person: full name, home address, phone number, email address, Social Security number, or biometric data. Data that seems harmless can become identifying in combination. A zip code plus a birth date plus a gender can be enough to single out most people in the United States.

Websites and apps collect data about you constantly. **Cookies** are small files a site stores on your device to remember you, track what you click, and keep you signed in. Third-party cookies follow you across different sites. **Location tracking** records where your phone goes. **Search and purchase histories** build a record of your interests. Much of this collection happens under privacy policies that few people read.

Data mining analyzes large collections of data to find patterns. A store can mine purchase histories and learn that buyers of one product often buy another. Data mining itself is neutral. The same techniques that recommend a movie also flag fraudulent charges.

Targeted advertising uses mined data to show you ads matched to your inferred interests. It is the business model behind most free online services. The service is free because advertisers pay to reach you. The trade is your data for their content, and the exam expects you to name that trade.

Trap. Removing names from a dataset does not make it anonymous. A dataset with names stripped can still identify people when combined with other data, such as location records or public profiles. Deleting your name from a record is not the same as making the record anonymous.

5.6 Protecting Yourself: Safe Computing

Safe computing is a set of habits that protect your devices and information from unauthorized access. The exam tests four practices by name. The next sections go deeper on how encryption works, who verifies a site's identity, how authentication layers protection, and which attacks these practices defend against.

PRACTICE	WHAT IT DOES
Strong passwords	Long passwords that are unique to each account. A password manager can generate and store them, so one breached site does not expose your other accounts.
Multi-factor authentication	Requires two or more kinds of proof: something you know, something you have, or something you are. It protects an account even if the password is stolen.
Encryption	Encodes data so it is unreadable without the key. Look for HTTPS and the lock icon in the address bar. It protects data from anyone who intercepts or steals it.
Software updates	Install patches promptly. Updates close security flaws that attackers exploit, and outdated software is one of the most common ways attackers get in.

Encryption protects data in two states, and the exam tests whether you match the protection to the threat. **Data in transit** is data moving across a network, such as a message traveling to a server. **Data at rest** is data sitting in storage, such as files on your laptop.

STATE	THREATS	PROTECTIONS
In transit	Interception on public Wi-Fi, eavesdropping on the network.	HTTPS or TLS, virtual private networks (VPNs).
At rest	Stolen device, server breach, unauthorized access to storage.	Full-disk encryption, strong device passwords, access controls.

Trap. A strong password does not protect data in transit. If you send a file over public Wi-Fi without encryption, anyone listening on the network can read it no matter how strong your password is. Passwords guard access to accounts and devices. Encryption guards the data itself.

5.6 Encryption: Symmetric and Asymmetric

The safe computing table said that encryption makes data unreadable without the key. There are two kinds, and the exam tests the trade-off between them. **Symmetric encryption** uses one shared secret key to both encrypt and decrypt, so both sides must hold the same key. It is fast, which makes it the right tool for large amounts of data. Its weakness is the **key-distribution problem**: sharing the key without anyone intercepting it.

Asymmetric encryption, also called **public-key encryption**, uses a key pair instead of a shared key. The **public key** is shared openly and can only encrypt. The **private key** stays secret and is the only key that can decrypt, so anyone can lock a message with your public key but only you can unlock it. The key-distribution problem disappears. The trade-off is speed. Asymmetric encryption is much slower, so it is a poor choice for bulk data.

HTTPS uses both, in a sequence the exam expects you to know. During the **handshake** that opens a secure connection, the browser and server use asymmetric encryption to agree on a shared secret over the insecure network. That secret becomes the **session key**, and everything after that is encrypted symmetrically with it, which is fast enough to keep up.

Trap. Asymmetric encryption does not protect everything just because it is harder to break. It is too slow for bulk data, so it handles only the handshake. When a question asks why a secure connection uses two kinds of encryption, the answer is that one solves key distribution and the other moves data quickly.

5.6 Digital Certificates and Certificate Authorities

A public key on its own does not prove who it belongs to. An attacker could hand you their public key while claiming to be your bank. A **digital certificate** closes that gap by binding a public key to a verified identity, such as a domain name, and carrying the issuer's digital signature and an expiration date. Before the handshake finishes, your browser checks the certificate: a trusted issuer's signature, a matching site name, and a date that has not expired.

A **certificate authority**, or CA, is the trusted organization that verifies the identity and signs the certificate. When a site owner requests one, the CA confirms the requester controls the domain, then issues the signed certificate that the site sends to every visitor. Your device ships with a list of CAs it trusts, and that list is what makes the whole chain work.

Trap. A certificate vouches for identity, not for honesty. The padlock icon means the connection is encrypted and the site proved it controls its domain name. It does not mean the site is safe, because attackers can obtain valid certificates for phishing sites. A padlock never proves a site is trustworthy.

5.6 Authentication: Strong Passwords and Multi-Factor Authentication

The safe computing table listed strong passwords and multi-factor authentication as separate practices because they defend an account in different ways. A **strong password** is long and unique to each account. Length matters more than clever substitutions, and uniqueness matters because breaches happen: when one site leaks its password database, attackers try those same passwords everywhere else. A **password manager** generates and stores a different long password for each account, so you only need to remember one.

Even a strong password is still a single kind of proof, something you know. **Multi-factor authentication** requires two or more different kinds of proof: something you know such as a password or PIN, something you have such as your phone or a hardware key, and something you are such as a fingerprint or face scan. The common second factor is a code from an authenticator app or text message. With MFA turned on, a stolen password alone cannot open the account, which is why the exam treats it as the defense that survives a password breach.

5.6 Cybersecurity Threats

Safe computing habits exist because specific attacks target your devices and accounts. Each attack below works by a distinct method, and the exam expects you to tell them apart.

THREAT	HOW IT WORKS	EXAMPLE
Phishing	A deceptive message impersonates a trusted source to trick you into revealing credentials or clicking a malicious link.	An email that looks like your bank warns of fraud and links to a fake login page.
Keylogging	Malware silently records every keystroke, capturing passwords as you type them without any visible sign.	A program installed by an infected download logs your banking password.
Malware	The umbrella term for any malicious software designed to harm a device, steal data, or give an attacker control.	Spyware that watches your activity and sends it to an attacker.
Computer virus	Malware that attaches to a host file or program and needs a person to open or run it before it can spread.	An infected email attachment that runs when you open it. A worm, by contrast, spreads on its own.
Ransomware	Malware that encrypts the victim's files and demands payment for the key that unlocks them.	A hospital's patient records are locked until the hospital pays the attacker.
DDoS attack	Many compromised devices flood a server with traffic at once, so legitimate users cannot reach it.	Thousands of hijacked devices overwhelm a retail site during a sale.

Trap. Match the defense to the attack. Strong passwords and MFA protect your accounts, but a keylogger captures keystrokes before they ever reach the login form, so password habits alone do not stop it. HTTPS encrypts your connection without proving a site is honest, so a padlock does not defeat phishing. Each defense in the safe computing table answers a specific attack.

Confusions That Cost Points

PAIR	HOW TO KEEP THEM STRAIGHT
Caused vs enabled	Caused means the innovation itself brought the change about. Enabled means it made the change possible. Social media enabled rapid fundraising. It did not cause people's generosity.
Open source vs public domain	Open source is copyrighted code shared under a license with conditions. Public domain has no copyright and no conditions to follow.
Creative Commons vs no restrictions	Every CC license requires attribution, and NC, SA, and ND add conditions. Only CC0 waives everything.
Plagiarism vs copyright infringement	Plagiarism is presenting someone else's work as your own, an ethical violation. Infringement is using copyrighted work without permission, a legal violation. Citation fixes the first, not the second.
Data in transit vs data at rest	In transit moves across networks and faces interception. Protect it with HTTPS or a VPN. At rest sits in storage and faces theft or breaches. Protect it with encryption and access controls.
Digital divide dimensions	Socioeconomic is about affording access. Geographic is about infrastructure reaching you. Demographic is about age, education, and background. Match the scenario to the dimension.
Crowdsourcing vs open source	Crowdsourcing enlists many people to contribute data or effort. Open source shares code under a license. A project can be both, but the terms describe different things.
Correlation vs causation	Two trends rising together does not prove the innovation caused the change. Look for the mechanism or a controlled comparison before claiming cause.
Symmetric vs asymmetric encryption	Symmetric encryption uses one shared key for both directions and is fast, but sharing the key securely is the hard part. Asymmetric encryption uses a public and private key pair and solves key distribution, but it is too slow for bulk data. HTTPS uses both.
Digital certificate vs certificate authority	A digital certificate binds a public key to a verified identity such as a domain name. A certificate authority is the trusted organization that verifies that identity and signs the certificate. The CA vouches for identity, not for safety or honesty.
Phishing vs keylogging	Phishing tricks you into volunteering your credentials through a deceptive message. Keylogging silently records your keystrokes without any trickery, so the victim does nothing unusual.
Computer virus vs malware	Malware is the umbrella term for all malicious software. A virus is one kind of malware that attaches to a host file and needs a person to open or run it before it can spread.
Strong password vs multi-factor authentication	A strong password is still a single factor, something you know. MFA adds a second kind of proof, something you have or something you are, so a stolen password alone cannot open the account.

Practice Questions

Original questions written for this guide in the style of the AP exam. Answers and explanations are on the next page, so complete the questions before checking them.

1. When a browser opens a secure HTTPS connection, the browser and the server first use public-key encryption to agree on a shared secret, then switch to encrypting the actual page data with that shared secret. Which statement best explains this design?

1. Symmetric encryption is too slow for any real use, so only public-key encryption can protect the session.
2. The shared secret is discarded because public-key encryption protects all of the data by itself.
3. Public-key encryption handles everything because it is more secure than symmetric encryption.
4. Public-key encryption solves the key-distribution problem during setup, and symmetric encryption then protects the bulk data because it is faster.

2. Which situation best illustrates the digital divide?

1. Two students own the same laptop model but prefer different browsers.
2. A student in a rural county cannot join video classes because no broadband provider serves her area, while students in the neighboring city can.
3. A student with home internet chooses to do homework at the library.
4. A school buys a tablet for every student, but some students leave theirs at home.

3. A bank trains a loan-approval model on decades of its own lending records, which reflect historical discrimination against certain neighborhoods. The model then denies loans in those neighborhoods at higher rates. This outcome is best explained by

1. biased training data producing biased outcomes.
2. the programmers intentionally coding discrimination into the model.
3. the model having too little data to learn from.
4. borrowers in those neighborhoods applying less often.

4. A student gets an email that appears to come from her college's financial aid office. It warns that her aid will be canceled unless she logs in through the link provided. The link opens a page that copies the real site's design and asks for her username and password. Which term describes this attack?

1. Keylogging, because the attacker records everything the student types.
2. Ransomware, because her financial aid is being held hostage.
3. Phishing, because the attacker used a deceptive message to trick her into giving up her credentials.
4. A computer virus, because the email carried malicious code into her inbox.

- 5.** A student finds a diagram licensed CC BY-NC for a class slideshow that she will post on her personal blog, which runs ads. Which statement is correct?
1. She may use it without crediting the creator because it is for school.
 2. She may edit the diagram freely because all Creative Commons licenses allow adaptations.
 3. She may use the diagram because Creative Commons means there are no restrictions.
 4. She should not use it on the ad-supported blog because the NC condition blocks commercial use.
- 6.** A developer includes an open-source library in a commercial product. Which statement is true?
1. The library's license may require attribution or sharing modifications, and she must follow it.
 2. The library is in the public domain, so no rules apply.
 3. Open source code has no copyright owner.
 4. She must pay the original author before using the library.
- 7.** A student uses a 15-second clip of a copyrighted song as background music in a video essay for class. A classmate says it is fine because the clip is short and the student cited the artist. Which statement is correct?
1. The use is automatically fair because the clip is short and cited.
 2. The use is automatically infringement because any use without permission is illegal.
 3. A court would weigh factors including the purpose of the use, the amount used, and the effect on the market for the song.
 4. Citing the artist gives legal permission to use the clip.
- 8.** A reporter working from a coffee shop needs to send sensitive interview notes to her editor. Which measure best protects the notes while they travel across the network?
1. Setting a strong password on her laptop.
 2. Sending the notes over an encrypted connection such as a VPN or HTTPS.
 3. Encrypting the laptop's hard drive.
 4. Deleting her browser history after sending.

Answer Key

- 1. D.** The handshake uses public-key encryption only to agree on the shared secret, because that solves the key-distribution problem. The bulk data is then encrypted symmetrically because symmetric encryption is fast. A is wrong because symmetric encryption is faster than asymmetric encryption, not slower. B is wrong because the shared secret is used: it becomes the session key that encrypts all the page data. C is the trap: a method being harder to break does not mean it is used for everything, and asymmetric encryption is too slow for bulk data.
- 2. B.** This is the geographic dimension of the digital divide: the student cannot buy service that does not reach her area. A is about preference, not access. C describes someone who has access and chooses not to use it. D is about device use habits after access was provided, not about a gap in access.
- 3. A.** The model learned the discrimination present in its training data and reproduced it. This is the standard bias pattern: biased data in, biased decisions out. B assumes programmer intent, which the scenario never mentions. C is wrong because the model had decades of data; the problem is what the data contains, not how much there is. D blames the applicants instead of the training data.
- 4. C.** The deceptive email impersonating a trusted office to steal credentials is phishing. A is wrong because keylogging silently records keystrokes; this attack tricks the victim into volunteering credentials through a fake page, which is a different method. B is wrong because ransomware encrypts files and demands payment; nothing here is encrypted or held for ransom. D is wrong because a virus is malware that needs a host file and a person to run it; this attack is social deception, not a spreading program.
- 5. D.** NC means noncommercial, and a blog that runs ads is a commercial use, so this use is blocked. A is wrong because every Creative Commons license requires attribution, including for school use. B is wrong because the ND licenses block adaptations; not every license allows them. C is the classic trap: Creative Commons always carries conditions.
- 6. A.** Open source code is still copyrighted, and its license sets conditions such as attribution or sharing modifications. B is the open source vs public domain trap: the library is licensed, not rights-free. C is wrong because open source code has an owner who chose the license. D is wrong because open source licenses permit use without payment; price is not the issue.
- 7. C.** Fair use is decided by weighing the four factors: purpose and character of the use, nature of the work, amount used, and effect on the market. A is wrong because no length of clip is automatically fair and citation is about plagiarism, not fair use. B is wrong because fair use is exactly the exception to permission. D is wrong because citing a source avoids plagiarism but does not grant legal permission.
- 8. B.** The notes are in transit across the coffee shop network, and an encrypted connection such as a VPN or HTTPS protects data in transit from interception. A protects access to the laptop, not data on the network. C protects data at rest on the hard drive, which is the wrong state. D does nothing to protect data while it travels.

When you check your answers, note which distinction each miss came from. Make a flashcard for that distinction and drill it spaced out over the next few days instead of rereading the whole section. If you missed one of these questions, the same distinction is worth practicing again in Rycal, where the Impact of Computing deck has flashcards for it and more practice questions use the same kinds of traps.

One-Page Recall Check

Say each answer out loud before you look back, and mark the ones you cannot finish. Anything you cannot say out loud yet belongs in your flashcard deck. In Rycal, add those items to the Impact of Computing deck and let spaced review bring them back over the next few days.

- Define a computing innovation and give one example each of a physical innovation, a software innovation, and a computing concept.
- Explain the difference between an innovation's purpose and its function.
- Describe one beneficial and one harmful effect of the same innovation, naming whether each affects society, the economy, or culture.
- Distinguish an intended effect from an unintended effect.
- Explain the difference between an innovation causing a change and enabling it.
- Define the digital divide and name its three dimensions, with an example of each.
- Name two efforts to close the digital divide and the dimension each one addresses.
- Explain how biased training data produces biased outcomes, using the hiring or lending pattern.
- Define crowdsourcing and give one citizen science example, plus one benefit and one limit.
- State what copyright, patents, and trademarks each protect.
- List the four Creative Commons license conditions and explain what each one restricts.
- Explain why open source software is not public domain.
- Distinguish plagiarism from copyright infringement and from fair use.
- Define PII and name three ways websites and apps collect data about you.
- Explain how data mining leads to targeted advertising.
- Name the four safe computing practices and what each one protects.
- Distinguish threats to data in transit from threats to data at rest, and name the protection for each.
- Explain the difference between symmetric and asymmetric encryption, and describe the role each one plays in an HTTPS connection.
- Explain what a digital certificate binds together, and state what a certificate authority does and does not vouch for.
- Describe how phishing, keylogging, ransomware, and a DDoS attack each work, and explain how they differ from one another.
- Explain what makes a password strong, and describe how multi-factor authentication protects an account even when the password is stolen.

Where to go next. Turn every missed item above into flashcards and drill them spaced out over several days rather than in one sitting. In Rycal, open the Impact of Computing deck under AP Computer Science Principles. The deck covers the terms in this guide, and its practice questions target the same traps named here. If you have a test date, add it in the Test Planner. You can also start your next review with a Brain Dump, then check what you missed against this guide.

Key terms for this unit

Computing innovation, Purpose and function, Intended and unintended effects, Society, economy, and culture, Digital divide, Computing bias, Training data, Crowdsourcing, Citizen science, Volunteer computing, Intellectual property,

Copyright, Patent, Trademark, Creative Commons, Attribution, CC BY, CC BY-SA, CC BY-NC, CC BY-NC-SA, CC BY-ND, CC BY-NC-ND, CC0, Open source, Proprietary software, Public domain, Open access, Plagiarism, Fair use, Personally identifiable information (PII), Cookies, Location tracking, Data mining, Targeted advertising, Strong password, Multi-factor authentication (MFA), Encryption, Symmetric encryption, Asymmetric (public-key) encryption, Session key, Digital certificate, Certificate authority, Phishing, Keylogging, Malware, Computer virus, Ransomware, Distributed denial-of-service (DDoS), Software update, Data in transit, Data at rest.

About this guide. Written for Rycal and aligned to the College Board AP Computer Science Principles course framework, Unit 5. All questions and explanations are original Rycal writing. Rycal is independent and is not affiliated with or endorsed by the College Board.