ANTI VIRUS SOFTWARE
Why Do I Need It?

- **What are the dangers to my computer?**

ADDWARE

Although mostly benign, adware can be annoying as it may cause popup ads to appear on your screen or browser and interrupt your work. More insidious adware may even try to track your private activities.

SURVEILLANCE

Surveillance malware is adware's natural companion, as often surveillance malware is designed to track your behavior so that someone can try to sell you stuff. But other surveillance malware might try to monitor your access to things like your bank account, with the goal of directly stealing your money. At a nation-state level, surveillance malware can be used for espionage.

Although nearly always bad, there are some legitimate use cases for surveillance software if, for example, you are employed at a company that needs to monitor what you do very closely for compliance purposes. If in doubt, check with your IT department.

KEY LOGGER

A close cousin to surveillance software, key loggers specifically try to track everything you type. This can lead to the capture of things like the passwords you use to log in to important websites.

VIRUS

A virus is designed to infect your system and then attempt to spread to other systems - it will often add itself to your documents and some programs and may even attempt to spread over your local network.

TROJAN

A Trojan, named after the Trojan horse, is something that appears to be benign, but once you let it in, it will compromise your system. The Trojan is designed to fool you into clicking on it to start it running, after which it will attempt to install a backdoor, run ransomware, steal data, and/or perform many other possible malicious actions.

ROOTKIT

Possibly the most insidious kind of malware, rootkits are designed to install themselves so deeply within your device's operating systems that you can't even see them - they will hide files, network connections, and any other indicators you can look at to remain stealthy. Rootkits are designed to dig deep and then stay on your system forever. Many low-cost antivirus software do not even check for rootkits. Don’t skimp on security. Invest in quality software to ensure protection.

PUP

A PUP (Potentially Unwanted Program) is something you probably don't want, but

you're not quite sure. PUPs often have some legitimate reasons for being on your system but usually also have annoying, privacy-threatening, or other potentially malicious features. For example, there are many games that use pop-up ads that are classified as PUPs.

DIALER

A dialer is an application that can cause your computer to call expensive toll lines and run up charges. These are less common today as most people use broadband, but you may run across them occasionally.

Don't Be Fooled by Imposter Scams

Fraudsters will do anything to be you. With Artificial Intelligence (AI) becoming more accessible, they now have even more—often indistinguishable—ways to try and scam you. Don't let them.

You can never be too safe with your information. If you're pressured to act fast, give personal or private information, send funds via a wire transfer, gift card, payment app or cryptocurrency, or told to keep the call a secret, you are talking to an imposter. Protect yourself and stop engaging immediately.

Review these top imposter scams so you can avoid falling for them:

Family-in-distress scam: Scammers use AI to clone your loved one's voice to request urgent emergency funds. Even if they sound distressed, hang up and call the family member to verify.

Charity scams: Posing as a real or fake charity, scammers request illegitimate donations from their targets. If you suspect a call is fraudulent, hang up and call the charity back using their legitimate phone number; do not simply redial.

Tech support scams: Fear is a great motivator. Imposter scammers use it as a tactic to get you to act quickly—or you'll be at great risk! Remember, tech support agents will never contact you by phone or text unless you request it.

Government scams: Unexpected contact from the IRS or Social Security office should be met with suspicion, as <u>government agents will contact you through the mail first, not by phone.</u>

- Majority of Americans Have Been Victims of Data Breaches. **Chances are all of us in this room have been affected**
- **August 16,2024**
- **National Public Data Breach:** As reported elsewhere by Tech.co, personal information belonging to **<u>2.9 billion individuals has been leaked</u>** on the dark web in a catastrophic data breach.
- National Public Data (NPD) was breached by hacking group USDoD. <u>Full names, addresses, dates of birth, phone numbers, and Social Security numbers were compromised in the breach</u>, which is likely to have affected most – if not all – US citizens.
- <u>Millions of email addresses were stolen by this and other data breaches</u>.

- Beware of fake emails; especially ones with attachments. If the sender is someone you know, reach out and ask if the person sent you something attached to an email.
  •Never click on a web link. It will take you down a dark path to trouble. The address most likely leads to a site that will infect your PC with Malware or Virus
- **Carefully examine the address of the sender kr202021@sanclar-mc.sch.id.**
- **The last two letters is the code for the country where the message originated. In this example, the email came from .id which is the code for Indonesia.**

I use Thunderbird as my email client.
Notice that Thunderbird tagged the emails as SPAM. This is a safety feature built into the software.
It is a free program available at https://www.thunderbird.net/en-US/download/

- Always check your antivirus software to make sure it is up to date.

- Use malware detection software such as Malwarebytes in addition to your antivirus software.
- Use a quality antivirus software package. Don't skimp on security.
- Make sure the software is set up to do an automatic scan of your system.
- If your software does not have an auto scan feature, then make sure you do a manual scan on a consistent basis.
- Make sure the software is set to do automatic checks for updates.
-

- HOW CAN YOU PROTECT YOURSELF
- Apply for annual Free Credit Report from the major credit bureaus.
- https://www.annualcreditreport.com/
- Experts recommend that anyone with concerns freeze their credit.
- You can freeze your credit by contacting the major credit bureaus, Experian, Equifax, TransUnion.
- Sign up for credit monitoring service.
- You can purchase additional protection through dark web monitoring services or identity theft monitoring tools.

- **Fake Virus Warnings**
- What is a fake virus?
- A fake virus alert, also known as fake virus software or rogue antivirus, is malware that appears to behave like real antivirus software but runs fake scans on your computer and displays fake virus warnings. Phony computer virus alerts make you think your device is infected with malware then trick you into clicking a link that could cause a real malware infection.
- A fake virus warning is a form of scareware that uses social engineering tricks to play on your emotions and cause panic. If you believe your device is infected with a computer virus, you might act without thinking and accidentally download harmful software.

- Fake virus warnings commonly appear on your screen as pop-ups warning you about some urgent malware threat and encouraging you to act immediately and download their product. Fake virus warnings can also appear as fake spyware warnings or fake system notifications.

- **What to do if you see a fake virus warning pop-up**

- If you think you've spotted a fake virus warning, here's how to deal with it:
- **Make sure the fake virus alert really is fake:** There are plenty of fakes out there, but don't forget that real infections do happen. If you think your computer or phone has an actual malware infection, use a trustworthy malware and virus removal tool.
- **Don't click on the pop-up:** Scareware plays on your emotions to make you act quickly and install something harmful. Don't fall for the apparently urgent warnings, and don't click on the pop-up. Also, look out for the "X" buttons. Phony virus pop-ups may use fake close buttons that can install actual malware on your device if you click.
- .Close your browser: To get rid of the ad, close your browser — don't click the "X" on a fake virus pop-up. To close your browser, open the Task Manager (use the keyboard shortcut: Ctrl + Shift + Esc) or right-click the browser in the task bar and select Close all windows.
- **Search the product name:** When in doubt, look up the name you see in the warning. If you can't find it online, or if the alleged company has terrible reviews, it's almost certainly a fake
- **Run an antivirus scan:** Fake virus pop-ups can result in real malware threats. Run a scan with a legitimate antivirus program to check for any malware.

- **Fake warnings can appear on your PC or your phone**
- Fake warnings often have poor grammar.
-

- **Look out for fake emails**
- Fake emails are the result of a data breach where your information is stolen then sold on the black market known as the "Dark Web"
- I became a victim of this when a data breach occurred in 2021.
- A company called Luxottica (manufacturer of eyeglasses) was breached and customer data was stolen. Including my name, address, and email.
- I now get tons of fake emails.

- **Look out for fake emails**
- Fake emails try to lure you into clicking on a link or attachment that contains a harmful virus or other identity stealing software.

- What Antivirus Software To Use?
- The market is full of software, all claiming to be the best.
- How can you be sure?
- If you do a google search on Top Ten Antivirus Software, you will get different results each day. This is because Google gets paid for listing software on its search results.
-
- Who gives you a real answer?
- AV-Comparatives
- AV-Comparatives is an Austrian independent organization that tests and assesses antivirus software, regularly releasing charts and reports that are freely available to the public and the media. Antivirus vendors must meet various requirements regarding trustworthiness and reliability in order to take part in the tests.

- AV-Comparatives issues relevant awards, based on antivirus software's comprehensive performance according to multiple testing criteria.
- It is also supported by the University of Innsbruck and other academic bodies from around the world, as well as by the Austrian Federal Government and the regional government of Tirol, Austria.
- https://www.av-comparatives.org
- This website leads to an independent testing organization that evaluates the leading antivirus software.

- **The Ratings Are Based On Real World Testing, Not A Lab Controlled Environment**

- AV Comparatives invites software developers to submit software for testing. Not all developers qualify. Antivirus vendors must meet various requirements regarding trustworthiness and reliability to take part in the tests.

- The tests use real world threats that are circulating on the internet and pose a real threat to the public.

-
- Based On My Own Experience Using The Products, Here Are My Favorites
- Malwarebytes Advanced Premium
- Acronis Cyber Protect
- Mc Afee
- Norton 360
- Although Vipre has good ratings, it is not an American company any longer. It has been sold to a German software company and both the product and customer service are not as good as they used to be.
- However, Be prepared to pay. These are premium products with a premium price.

- Useful Links
- https://www.iban.com/country-codes
- https://www.thunderbird.net/en-US/download/

Questions?