

Online Security and Privacy



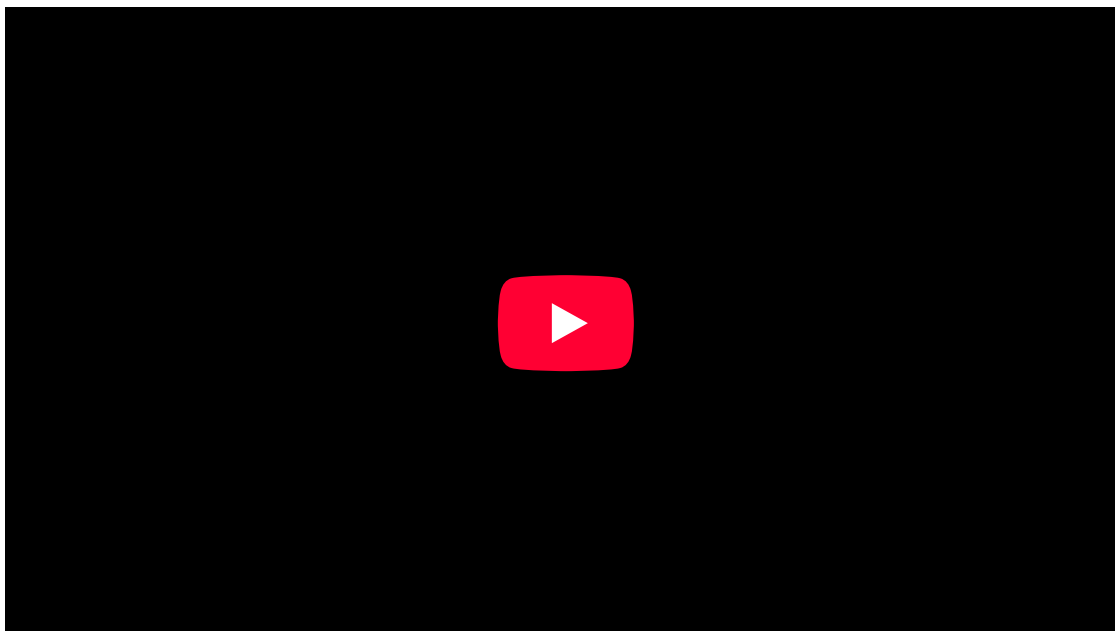
Summary

Staying safe and responsible online requires smart habits.

- First, **think before you share**—your posts can be permanent and affect your **reputation**. Be mindful of who can see your content, as it can impact opportunities like jobs or college.
- Second, **protect your stuff** by using **strong passwords** with a mix of letters, numbers, and symbols. Never share passwords except with a trusted adult, and always log out from **public** computers.
- Third, **know and use your settings** to keep personal **information** private. Adjust **security settings** on each platform to control who sees your **posts**.
- Fourth, **avoid scams** like phishing attempts that trick you into giving away **passwords** or personal details. Be **suspicious** of offers that seem too good to be true.
- Lastly, **be positive**—encourage kindness online, report negativity, and use the **internet** to make a difference.

By following these tips, you can create a **safe**, responsible, and enjoyable online experience.

Tip 1: Think Before You Share



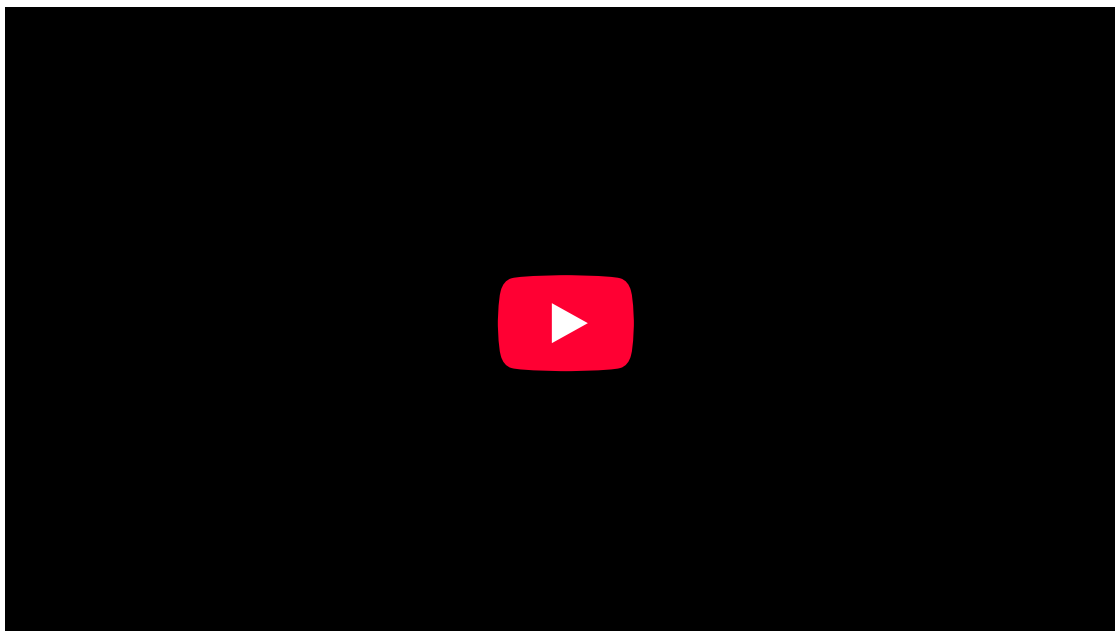
Think before you share! The **web** connects us all and allows us to **share** in ways we have never before been able to. Whether through **social media** posts, comments, or even videos, we can reach friends near and far with just a **click**. But what you share on the web and who you share it with can end up saying a lot about you—and can become a part of your **life story**. You can't control information once it's out there in the world.

What you post or send can easily be **forwarded**, copied, or found by other **internet users**, including strangers or people you know who aren't necessarily your friends. Other people's impressions of you can change based on what you share. Posting **inappropriate** information can have **negative** consequences you may not have considered. This can impact your place on the soccer team, summer job opportunities, and even one day, what **college** you go to.

The **internet** is an awesome tool for having fun and making new friends. But with great power comes great responsibility. So use your power for good. You can just as easily lose friends as make them, based on how you manage your **reputation** online.

So don't forget—to **think before you share**.

Tip 2: Protect Your Stuff



Most of us have things on the **web** that we want to keep **safe**. One of the best ways to do this is by setting **strong passwords** on all your accounts. By knowing how to create strong passwords, you can further safeguard your **personal information**.

So, how do you create a really strong password? First, use at least **eight characters**—the longer your password is, the harder it is to guess. Second, mix **letters, numbers, and symbols**. Third, make it different for each site.

Once we know how to set a strong password, we need to learn how to **remember** it. We recommend picking a favorite book title, sports team, song, or phrase to help you build a strong password. Don't **share** your password unless it's with a parent or trusted adult. Like the key to your house or the combination to your locker, passwords protect things that are valuable to you and shouldn't be shared.

Protecting your **information** online also means logging out of websites, programs, and applications when you're using a **public** or shared computer. If you don't log out, someone else could access your accounts and personal information.

So always remember to **protect** your stuff.

Tip 3: Know and Use Your Settings



Why do you need to understand **settings**? Because not all **information** people post online is meant to be seen by absolutely everyone. Some information should be kept **private** or shared with a smaller audience.

Just like in the real world, you share different things with different people. You can share some **pictures** with family and friends, but think carefully about what you share with everyone else. **Security settings** can help you control who can see your **posts**, making it easier to keep your information **safe**.

Most sites will have **settings** buttons where you can easily find them. However, remember that they can be in different places on each site you use. The wrong **settings** can expose your **personal** details to more people than you intended.

So always remember—to **know and use your settings**.

Tip 4: Avoid Scams

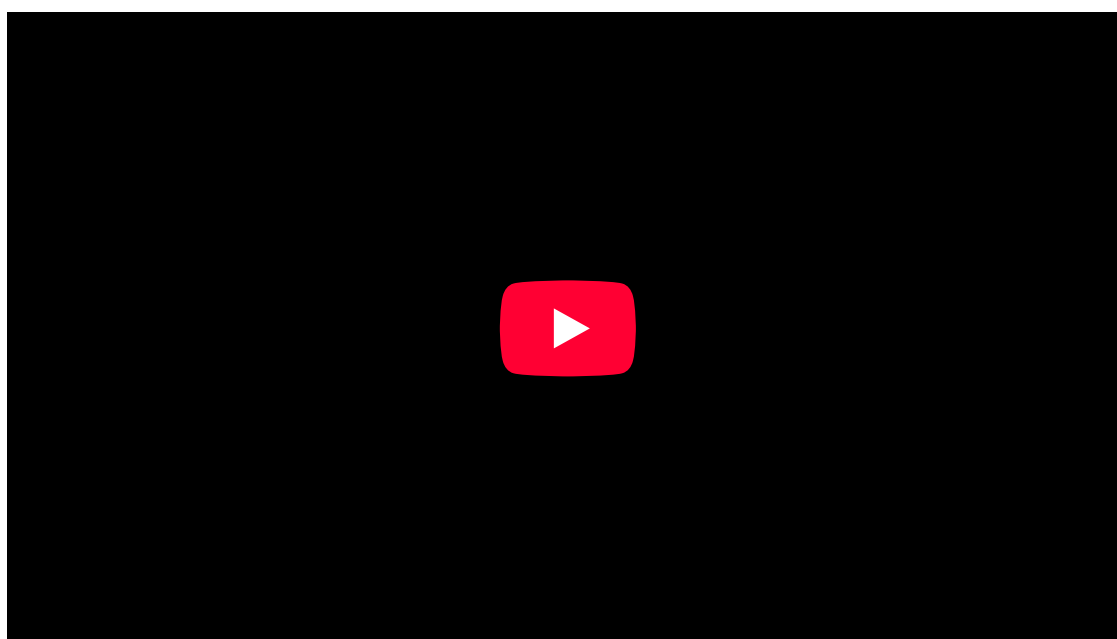


Everyone knows you should never take **candy** from a **stranger**, right? The same principle applies **online**. If someone offers you candy, new **shoes**, a **tablet**, or tells you that you won a **trip** to Hawaii, you should be **suspicious**.

This might seem harmless, but these could be very dangerous ways to lure you in and steal your **passwords** or even your **identity**. This is known as **phishing**. Phishing is the act of attempting to acquire **information** such as usernames, passwords, and personal details by pretending to be a **trustworthy** source.

By knowing how to identify a **phishing scam**, you can protect yourself and your **personal** information. When in doubt, ask a **parent**, teacher, or trusted adult. So be **aware**, and avoid scams.

Tip 5: Be Positive



Being **positive** online is essential. Everyone, including **students**, is responsible for creating a great online **experience**. There are many ways, big and small, to contribute to this every day. A small positive **action** can make a big difference—leave an encouraging **comment** or send someone a thank-you **text**. These gestures are quick and easy, but they can have a lasting **impact** on someone's day. Plus, when you do something positive, you **inspire** others to do the same.

However, the opposite is also true. A little **negativity** can spread and turn into something big and harmful online. If you see someone being mean, talk to an **adult** or take charge and **report** it yourself. Only by taking **action** can we create **change** for ourselves and those around us, both online and in the real world. Everyone can be a **leader** and set a good **example** on the internet.

The **digital** world offers countless **opportunities** to do amazing things. You can use the **web** to explore the world around you, answer important **questions**, and solve big **problems**. The only question is: how are you going to **change** the world?

So set a good **example**—and be **positive**.

Glossary

English	Español	Example usage in context
access	acceso	Make sure only you have access to your account.
account recovery	recuperación de cuenta	Use the account recovery option if you forget your password.
action	acción	Take action immediately if you detect suspicious activity.
adult	adulto	Ask a trusted adult if you're unsure about something.
alert	alerta	The security alert will notify you about unauthorized login attempts.
analysis	análisis	Perform a security analysis to protect your account.
answer	respuesta	Don't answer emails from unknown sources.
ask	preguntar	If you're unsure about privacy, ask an expert.
awareness	conciencia	Awareness about privacy is key when using social media.
avoid	evitar	Avoid sharing personal information on insecure sites.
background	contexto	The context in which you share information can affect your privacy.
backup	copia de seguridad	Create a backup of your important files.
breach	brecha	The data breach exposed users' personal information.
build	crear	Build strong passwords to protect your account.
candy	dulce	Don't accept " candy " from strangers online, it could be a trick.
change	cambiar	Change your password regularly for better security.
click	hacer clic	Don't click on suspicious links in emails.
comment	comentario	Leave a respectful comment and avoid sharing personal data.
consequences	consecuencias	The consequences of a privacy breach can be serious.
connection	conexión	Make sure your internet connection is encrypted.
consent	consentimiento	Ensure you get consent before sharing someone else's information.
control	control	You have control over who sees your information on social media.
create	crear	Create a profile with minimal personal information to protect your privacy.

English	Español	Example usage in context
data	datos	Protect your personal data from hackers.
data breach	filtración de datos	A data breach can expose your personal information.
deactivate	desactivar	Deactivate your account if you no longer wish to use it.
detail	detalle	Don't include personal details in public posts.
details	detalles	Make sure your account details are kept private.
device	dispositivo	Keep your device secured with a password.
digital	digital	The digital world has both risks and benefits.
encryption	cifrado	Encryption ensures that no one can read your messages without permission.
encryption key	clave de cifrado	Keep your encryption key safe.
example	ejemplo	A good example of security is using different passwords for each account.
explore	explorar	Explore secure websites to gather information.
firewall	cortafuegos	The firewall protects your network from unauthorized access.
forward	reenviar	Don't forward emails from unknown sources.
friend	amigo	Make sure your online friends are trustworthy.
fun	diversión	Have fun online, but always keep security in mind.
good	bueno	It's good to regularly update your privacy settings.
harm	daño	A cyber attack can cause harm to your data and devices.
hacker	hacker	Hackers try to steal your personal information.
identity	identidad	Protect your identity from being stolen.
impact	impacto	A security breach can have a serious impact on your data.
information	información	Share personal information only with trusted people.
internet	internet	Browse the internet safely using secured networks.
key	clave	Your account key should be unique and hard to guess.
leader	líder	A leader in cybersecurity knows how to protect systems.
log out	cerrar sesión	Always log out when using a public computer.
locker	taquilla	Store your passwords securely in a safe place.
lose	perder	If you lose your phone, immediately lock all your accounts.
manage	gestionar	Manage your privacy settings for better security.

English	Español	Example usage in context
malware	malware	Malware can steal your information without you noticing.
mix	mezclar	Don't mix simple passwords with more complex ones.
negative	negativo	Negative content online can damage your reputation.
opportunity	oportunidad	Don't miss the opportunity to improve your account security.
password	contraseña	Make sure your password is at least eight characters long.
password manager	gestor de contraseñas	Use a password manager to keep your passwords secure.
personal	personal	Don't share personal information with strangers.
phishing	suplantación de identidad	Phishing is when attackers impersonate a trusted source to steal your data.
post	publicación	Think carefully before posting something online.
private	privado	Keep your information private to avoid exposure.
privacy	privacidad	Privacy is essential for protecting your personal data.
protect	proteger	Protect your devices with strong passwords.
public	público	Make sure your profile is only visible to friends, not the public .
public key	clave pública	The public key is used to encrypt your messages.
question	pregunta	Always ask questions about how your data is being handled.
profile	perfil	Customize your profile to control what information is shared.
protection	protección	Protection of your account is key to preventing data theft.
reputation	reputación	Keep a good reputation online to avoid misunderstandings.
report	informar	Report any suspicious activity to the administrators.
risk	riesgo	Weak passwords increase the risk of a cyber attack.
risk assessment	evaluación de riesgos	Conduct a risk assessment to prevent security issues.
safety	seguridad	Online safety starts with good practices.
scam	estafa	Don't fall for scams promising unexpected prizes.
security	seguridad	Account security should be your top priority.

English	Español	Example usage in context
secure	seguro	Make sure your connection is secure before sending sensitive information.
secure connection	conexión segura	Always use a secure connection when accessing sensitive information.
settings	configuraciones	Review your privacy settings to protect your account.
share	compartir	Share only necessary information to protect your privacy.
setting	configuración	Change your privacy settings if you don't want everyone to see your profile.
stranger	extraño	Don't talk to strangers online or share your data.
strong	fuerte	A strong password is crucial for protecting your account.
suspicious	sospechoso	Be suspicious of emails asking for your personal information.
system	sistema	The security system protects your accounts from unauthorized access.
team	equipo	Work together as a team to improve network security.
threat	amenaza	The threat of a cyber attack is increasing every day.
trust	confianza	Trust is important online, but always verify the sources.
trustworthy	confiable	Ensure the people you interact with online are trustworthy .
two-factor authentication	autenticación en dos pasos	Enable two-factor authentication for an extra layer of security.
update	actualizar	Keep your applications updated to avoid vulnerabilities.
use	usar	Use strong, unique passwords for each website.
web	web	The web is full of risks, but also offers many opportunities.
world	mundo	The digital world offers both opportunities and risks.
world wide web	red mundial de internet	The world wide web connects people from all over the world.
lockdown	bloqueo	Account lockdown prevents unauthorized access to your data.
notification	notificación	You'll receive a notification if someone tries to access your account.
track	rastrear	Websites can track your online activity.