ALTRIST ENERGY
Smart Saving Smart Energy

Catbytes Digital Community

# Free Digital Learning Sessions

**** SYSTEM ERROR: 1X00000001 (2X00000002, 3X00000003, 4X00000004)
EMERGENCY_SYSTEM_RESTART
Driver error_1x00000001_6.12.dll_missing_fatal_system_error
SYSTEM RESTART 55% COMPLETED

ALTRIST ENERGY
Smart Saving Smart Energy

Catbytes
Digital
Community

# Staying Safe Online

**** SYSTEM ERROR: 1X00000001 (2X00000002, 3X00000003, 4X00000004)
EMERGENCY_SYSTEM_RESTART
SYSTEM RESTART 55% COMPLETED

# Smartphones - Staying Safe Online

## What we are going to cover:

- Safe Use of Browsers
- Online Safety
- How to check if website is safe
- Password Manager
- Safe Online banking
- Online Scams - Basics

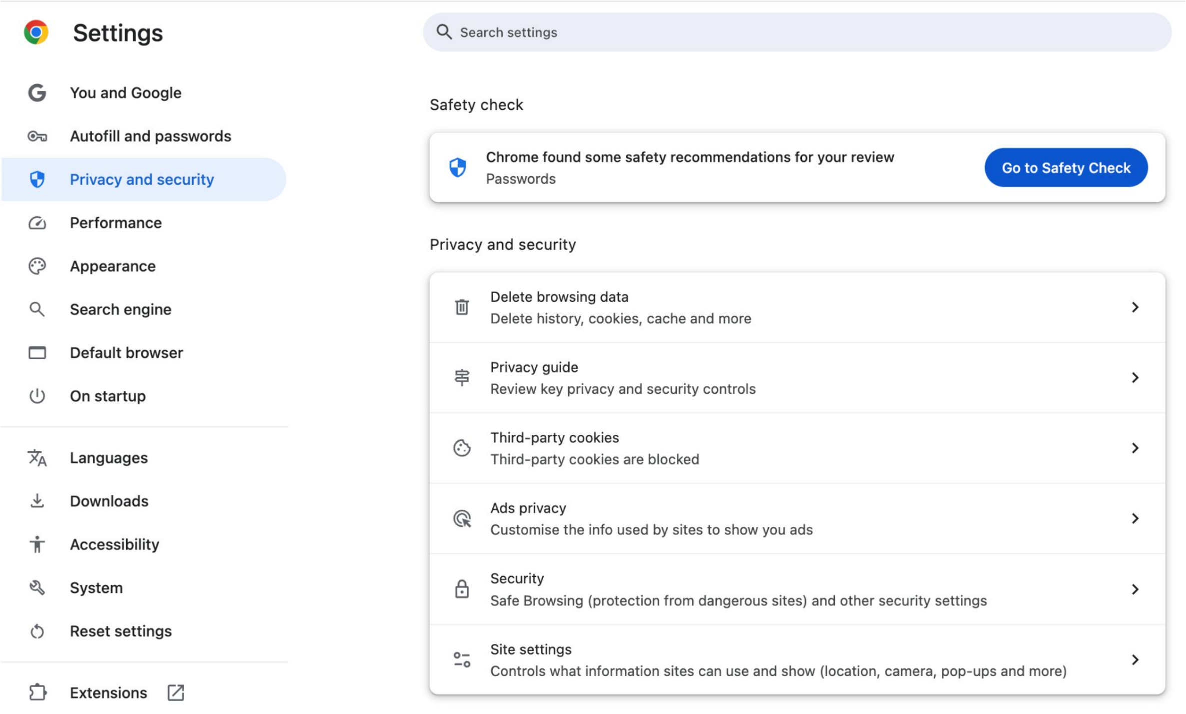
# Smartphone - Staying Safe Online

## Safe Use of Browsers:

- The most common internet browsers  e.g. Google Chrome, Safari, Microsoft Edge enable you to **manage your settings** such as allowing and blocking selected websites, blocking pop ups and browsing in private. Visit the security and privacy section of their websites.
- Always ensure that you are running the **latest version** of your chosen browser and **install the latest updates**
- Always remember to **log out** of a **secure website** when you have completed your transaction, and before you close the browser.

# Smartphone - Staying Safe Online

## **Safe Use of Browsers (cont):** Example of browser privacy/security settings - Chrome



Settings

Search settings

- You and Google
- Autofill and passwords
- Privacy and security
- Performance
- Appearance
- Search engine
- Default browser
- On startup
- Languages
- Downloads
- Accessibility
- System
- Reset settings
- Extensions

Safety check

Chrome found some safety recommendations for your review
Passwords

Go to Safety Check

Privacy and security

Delete browsing data
Delete history, cookies, cache and more

Privacy guide
Review key privacy and security controls

Third-party cookies
Third-party cookies are blocked

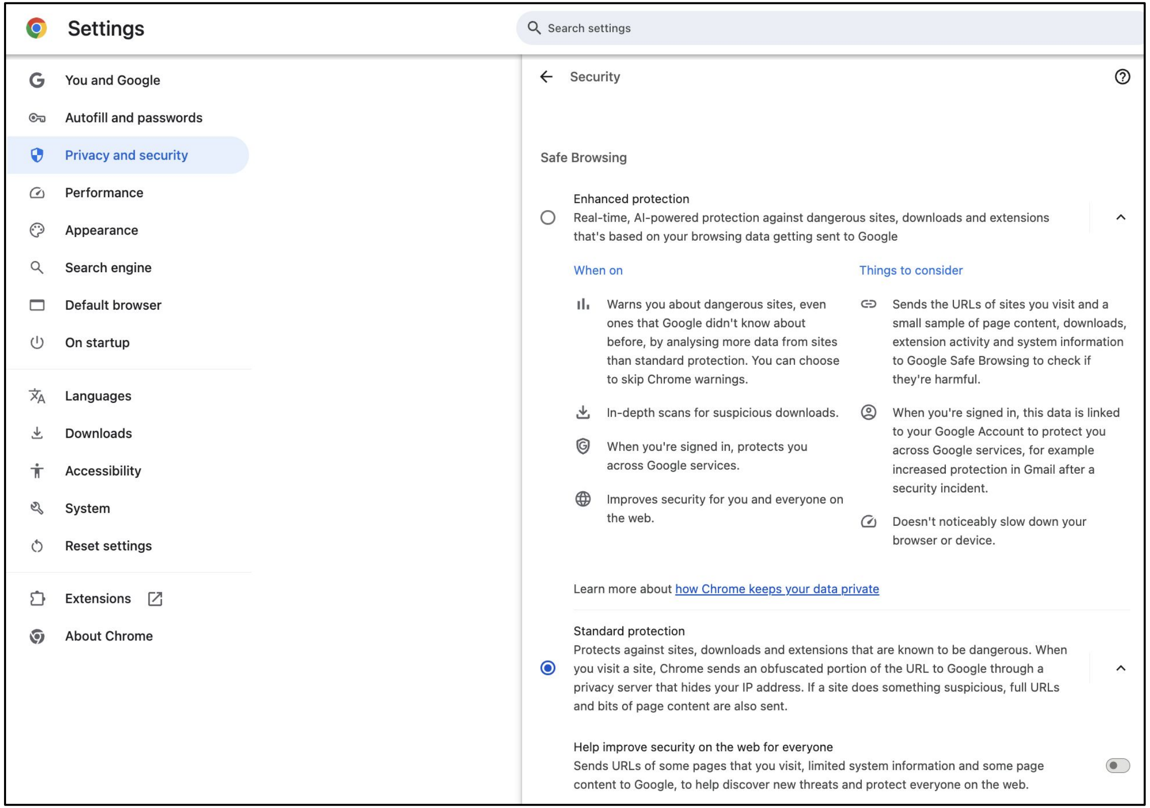
Ads privacy
Customise the info used by sites to show you ads

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site settings
Controls what information sites can use and show (location, camera, pop-ups and more)

# Smartphone - Staying Safe Online

## **Safe Use of Browsers (cont):** Example of browser privacy/security settings - Chrome



Settings

Search settings

- You and Google
- Autofill and passwords
- Privacy and security
- Performance
- Appearance
- Search engine
- Default browser
- On startup
- Languages
- Downloads
- Accessibility
- System
- Reset settings
- Extensions
- About Chrome

Security

Safe Browsing

○ Enhanced protection
Real-time, AI-powered protection against dangerous sites, downloads and extensions that's based on your browsing data getting sent to Google

When on

- Warns you about dangerous sites, even ones that Google didn't know about before, by analysing more data from sites than standard protection. You can choose to skip Chrome warnings.
- In-depth scans for suspicious downloads.
- When you're signed in, protects you across Google services.
- Improves security for you and everyone on the web.

Things to consider

- Sends the URLs of sites you visit and a small sample of page content, downloads, extension activity and system information to Google Safe Browsing to check if they're harmful.
- When you're signed in, this data is linked to your Google Account to protect you across Google services, for example increased protection in Gmail after a security incident.
- Doesn't noticeably slow down your browser or device.

Learn more about how Chrome keeps your data private

● Standard protection
Protects against sites, downloads and extensions that are known to be dangerous. When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.

Help improve security on the web for everyone
Sends URLs of some pages that you visit, limited system information and some page content to Google, to help discover new threats and protect everyone on the web.

# Smartphone - Staying Safe Online

**Online safety:** https://www.getsafeonline.org/resources/videos/

When browsing or shopping online it is **very important** to shop and browse safely!

- **Avoid** clicking on **links in emails or messages**. Criminals can use these links to capture your information. **Always visit an organisation's website directly** from your browser.
- **Be aware** of the risks of browsing online such as **malware & scams** particularly in public spaces
- **Always** use **secure internet connections** and try and **avoid free wifi hotspots**
- **Use strong** and **unique passwords** to prevent unauthorised access to your data and accounts
- **Only use secure websites** (they will have a padlock icon & 'https://' in the website address) and only make purchases from reputable sites
- **Never** use **fake websites** or ones that look suspicious e.g. have **misspelling in the website address**

# Smartphone - Staying Safe Online

## Online safety (cont):

- **Turn** on **2-step verification** to add an extra layer of security (in addition to password) to any accounts that have your personal or financial information *e.g. code sent via SMS or fingerprint*
- **Don't** use **public Wi-Fi** to access accounts that have your personal or financial information. *e.g. bank accounts*
- If your web browser flags that a website is '**not secure**' do not visit or use
- **Be aware** of what personal information you share on social media, online forums etc..
- **Use security software** (usually built into your smartphone e.g. iPhone & Samsung - go to 'Settings' app) and keep Software up to date.
- **For added protection** there are **reputable third party apps** that you can **install** on your smartphone e.g. Norton 360, Bitdefender Mobile Security

**Useful sources for staying safe online!:**

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

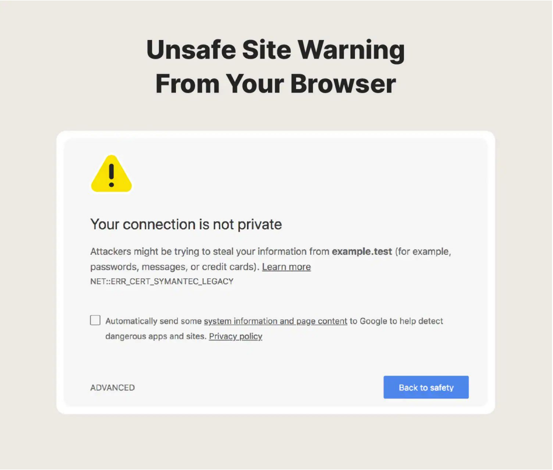
https://www.getsafeonline.org/

# Smartphone - Staying Safe Online

## How to Check if a Website is Safe

- **Most browsers** will **alert** you with a **warning** if a website is unsafe.
- If you see one of these warnings, **close the window** or click "**back to safety**" to avoid a potentially unsafe site.
- Look to see if there is a SSL Certificate. This is a digital certificate that certifies a website is legitimate and encrypts personal information.

[https://us.norton.com/blog/how-to/check-if-a-website-is-safe](https://us.norton.com/blog/how-to/check-if-a-website-is-safe)



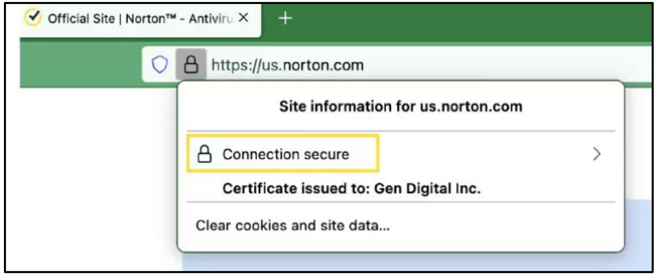
**Unsafe Site Warning From Your Browser**

Your connection is not private

Attackers might be trying to steal your information from **example.test** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_SYMANTEC_LEGACY

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy



**Site information for us.norton.com**

Connection secure

**Certificate issued to: Gen Digital Inc.**

Clear cookies and site data...

# Smartphone - Staying Safe Online

## Password Manager

Having **separate passwords** for your online accounts  **is important** and provides even **more security.** But with so many online accounts, creating and remembering them is very hard!! Using a **password manager** can help**!**

- These are usually **built into your  smartphone or browser** e.g. Google, Safari
- **iPhone** = ‘iCloud Keychain’. **Android** = ‘Google Password Manager’.
- A password manager automatically **stores passwords safely/securely** for apps and websites meaning you <u>won’t need to remember them</u> !
- Your **password** will **automatically appear** when you **log in** to your account
- It will alert you if password has been <u>breached</u> or <u>leaked!</u>
- <u>Provides ‘2 step verification’ to protect your password manager</u>

**Do not save passwords on shared devices!!**

# Smartphone - Staying Safe Online

## Password Manager (cont)

If you prefer to manage passwords by writing them down then it is **important to:**

- Keep written passwords in journal or book in a safe place!
- Make sure passwords are **not predictable or guessable**. And use a **strong and separate** password for your **email account**.
- Make sure you are **not breaking the terms and conditions of the service** you are creating a password for ! *e.g. some online banking services do not allow passwords to be written down!*
- **Be careful who you share your passwords with and whether they really need access to them!**

# Smartphone - Staying Safe Online

## Safe Online (Mobile) Banking:

- **Only download** banking apps from your smartphone’s **official app store** as they are vetted.
- **Always** use your banks official website & look for **‘https’** at the beginning of the address and the padlock symbol.
- **Use the security features** offered by your bank or built into your phone. E.g. biometrics such as fingerprint or 2 factor authentication
- **Never share** personal banking information i.e Pin or Online Password (***Remember: your bank will never ask for these in full***)
- **Always log out** of your **banking app or mobile website** when you have finished using it. (***Note:*** *Closing the app or web page or turning off your device may not be sufficient*.)

# Smartphone - Staying Safe Online

## Online Scams (basics):

Online scams are fraudulent schemes conducted through the internet, often using emails, texts, or fake websites. Common online scams include:

- **Phishing -** uses fake links and urgent messages to steal your login details
- **Romance scams -** where a fraudster creates a fake online persona to manipulate someone into sending money
- **Fake government websites:** Scammers create copycat websites that look like official government sites, charging you for services you can get for free or cheaper directly from the government
- **Unexpected money/lottery scams:** You're told you've won a prize, lottery, or inheritance but must pay an upfront fee, tax, or other cost to claim it.

**Beware of emails, texts or phone calls** claiming to be from your **bank** or the **police** claiming there is a **problem with your account** and requesting your login or other confidential details

# Smartphone - Staying Safe Online

**Here are some useful videos:**

Shopping online: https://www.getsafeonline.org/resources/videos/

Phishing scam: https://www.getsafeonline.org/resources/videos/

Online banking scam: https://www.getsafeonline.org/resources/videos/

# Thank you

# Any Questions?