DARTS: Deceiving Autonomous Cars with Toxic Signs

Presented by Miles Grant

Researchers

01

Chawin Sitawarin
Princeton University
Princeton, NJ, USA

02

Arjun Nitin Bhagoji
Princeton University
Princeton, NJ, USA

03

Arsalan Mosenia
Princeton University
Princeton, NJ, USA

04

Mung Chiang
Princeton University
Princeton, NJ, USA

05

Prateek Mittal
Princeton University
Princeton, NJ, USA

Background

Attacks on Machine Learning Systems

Machine learning systems typically have two phases, a training phase and a test phase.

A number of powerful attacks on the test phase of ML systems used for classification have been developed over the past few years.

These attacks have also been shown to work in black-box settings. These attacks work by adding carefully-crafted perturbations to benign examples to generate adversarial examples.

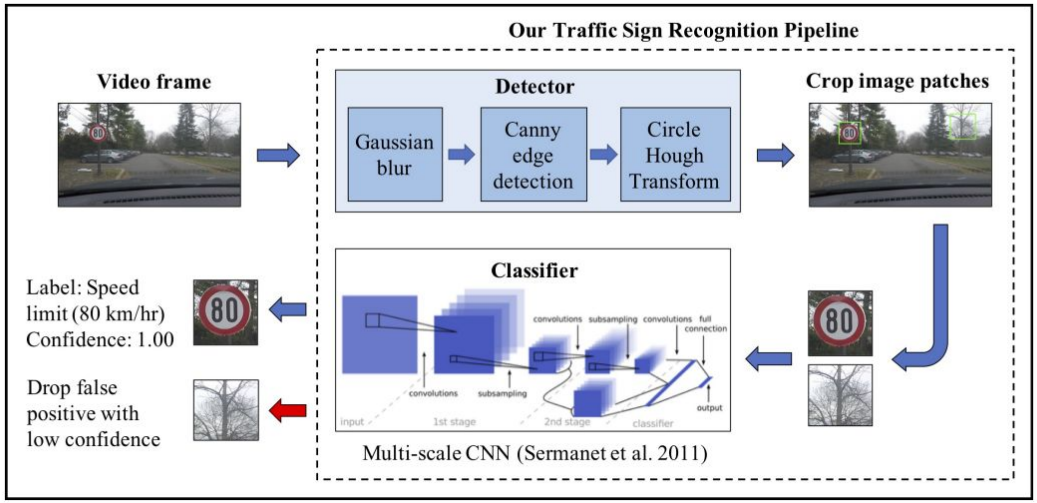
ML for Sign Recognition

The commonly-used traffic sign recognition pipeline used in the paper consists of two stages: detection and classification.

The shape based detector uses the circle Hough transform to identify the regions of a video frame or still image that contain a circular traffic sign.

The classifier outputs confidence scores for all output classes to determine whether the input is a traffic sign and assign its label. The label with the highest confidence is chosen as the final output only if its confidence is above a certain threshold.

Traffic Sign Recognition Pipeline



Attack Overview

Generate a Mask and Resize

The attack generates a mask to isolate the sign from the background.

The original image and mask are resized to the input size of the classifier.

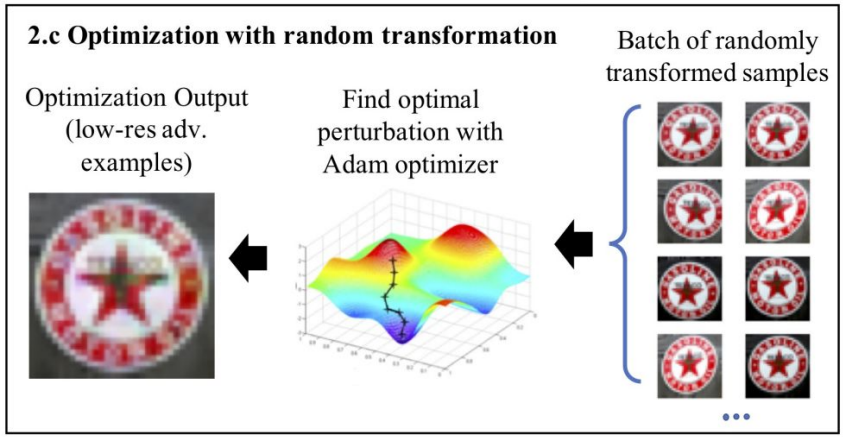
01

Optimize with Random Transformation

The attack runs an optimization algorithm to generate the perturbation.

The algorithm is run on a number of randomly transformed samples.

02

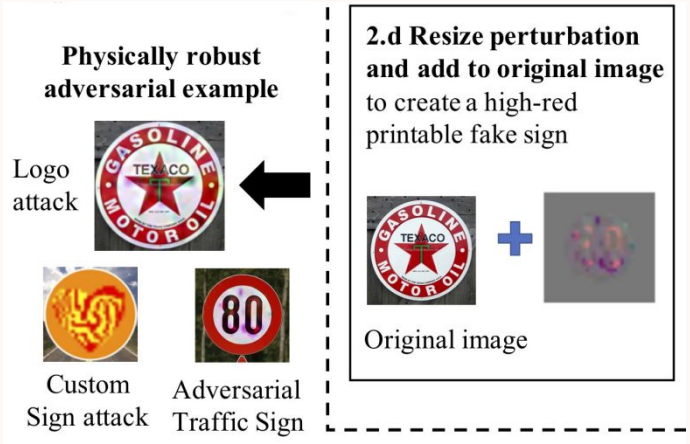


Resize and Add to Original Image

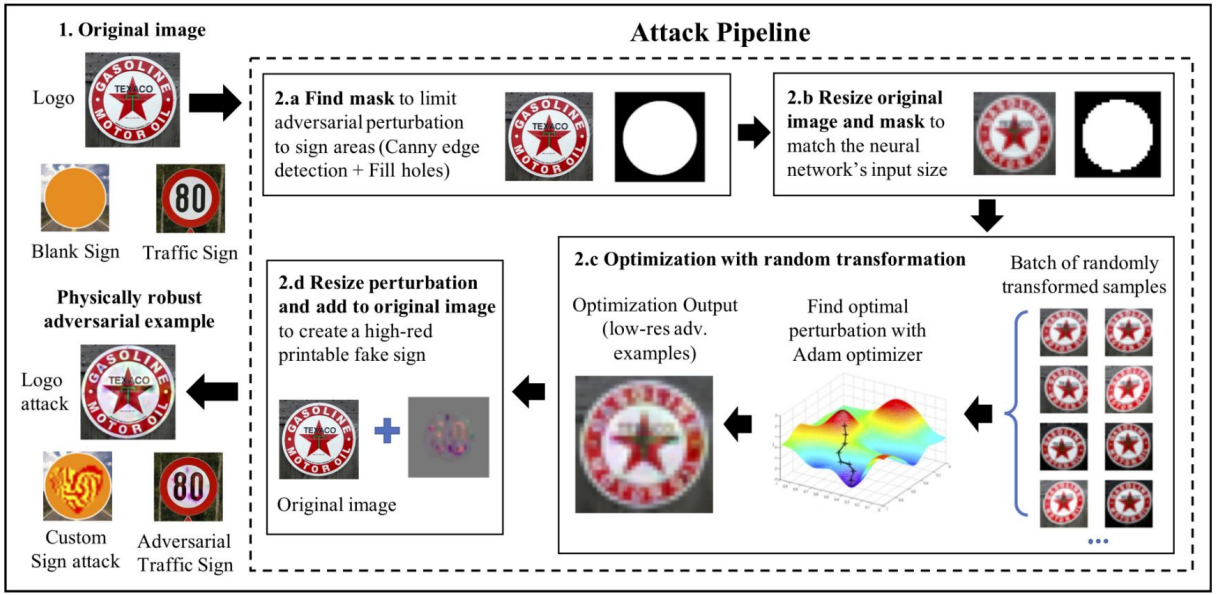
The output perturbation is resized to a high resolution and added to the original image.

This perturbation can be printed to create a physical toxic sign.

03



Attack Pipeline



Attack Types

In vs. Out-of-Distribution Attacks

Out-of-Distribution Attacks

Starts with an out-of-distribution image (not a traffic sign) and generates a targeted adversarial sign from it.

In-Distribution Attacks

Images of traffic signs are modified using imperceptible perturbations such that they are classified as a different traffic sign.

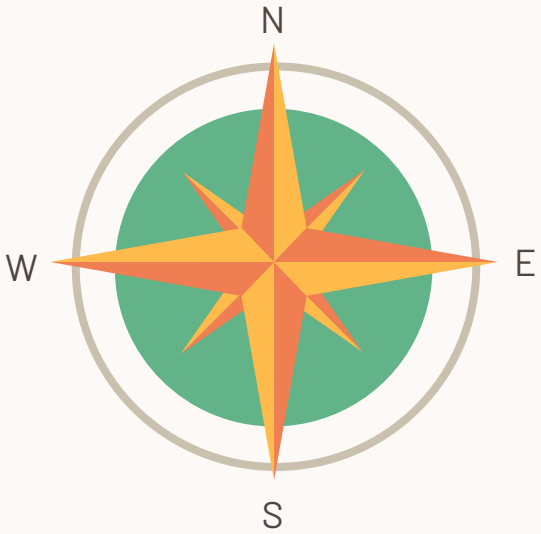
Out-Of-Distribution Attacks

Logo Attacks

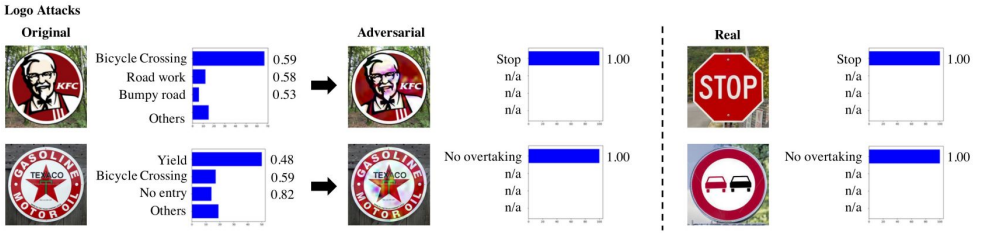
Images of commonly found logos are modified such that they are detected and classified with high confidence as traffic signs.

Custom Sign Attacks

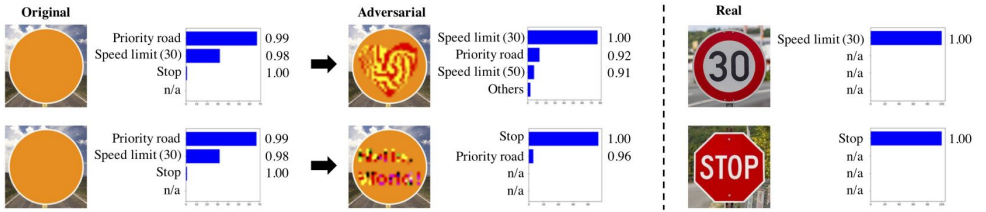
The adversary creates a custom sign that is adversarial starting from a blank sign.



Out-of-Distribution Attacks



(a) Classification of Logo attack examples. The adversarial examples are classified with high confidence as a real traffic sign, in spite of being out of the dataset.



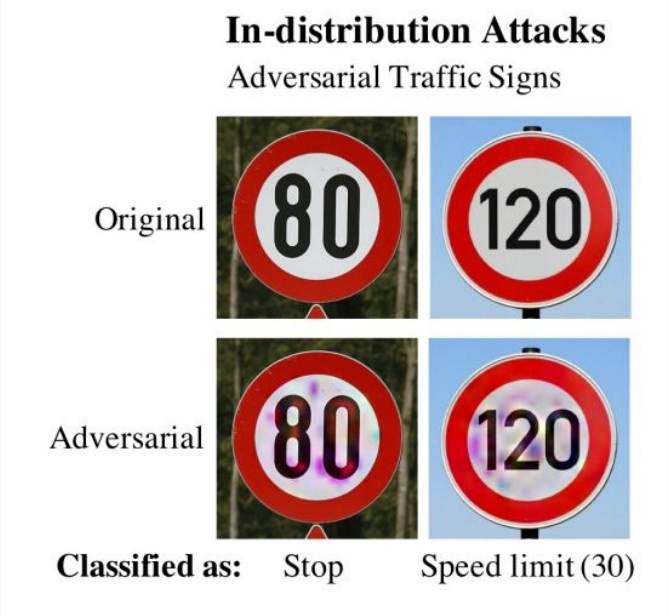
(b) Classification of Custom Sign attack examples. The adversarial examples are classified with high confidence as a real traffic sign, in spite of being custom made signs.

In-Distribution Attacks

In this attack, images of traffic signs are modified using imperceptible perturbations such that they are classified as a different traffic sign.

This attack is similar to attacks carried out in most previous work in both the virtual and physical settings.

The authors include it in the paper to demonstrate that their attack pipeline works in this setting as well.



Attack Videos

Lenticular Printing Attacks

Lenticular Printing

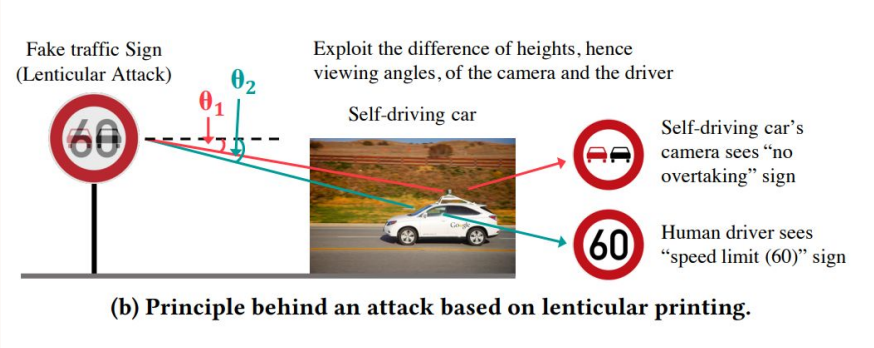
The authors exploit a multistep process, known as lenticular printing, that involves creating a special image from at least two existing images, and combining it with an array of magnifying lenses.

Lenticular printing relies on an optical phenomenon and has been traditionally used in photography and visual arts to generate 2-D images that can offer an illusion of depth and be changed as the image is viewed from different angles.

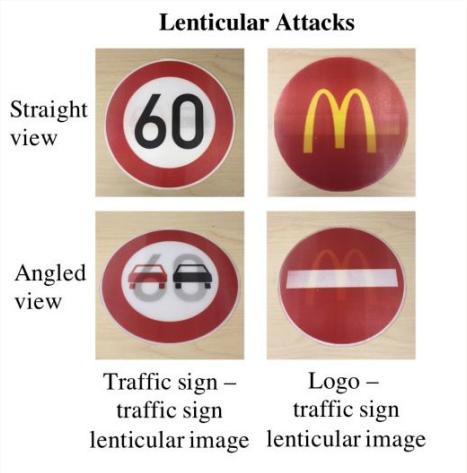
Lenticular Printing Attacks

The human driver and the vehicle-mounted camera observe the environment from two different observation angles.

The researchers create special traffic signs that appear differently from different observation angles.



(b) Principle behind an attack based on lenticular printing.



Attack Success

Real-World Attack Success Rates

Attacks	White Box (avg. confidence)	Black Box (avg. confidence)
In-Distribution (auxiliary traffic data)	92.82% (0.9632)	96.68% (0.9256)
Out-of-Distribution (Logo)	52.50% (0.9524)	32.73% (0.9172)
Out-of-Distribution (Custom Sign)	96.51% (0.9476)	97.71% (0.9161)

Limitations

Adversarial Example Detectors

While detection based defenses are ineffective against In-Distribution white-box attacks, it is is not known as to how they will perform against Out-of-Distribution attacks.

Synthesis of Sensor Inputs

While the computer vision subsystem is the only one able to recognize a traffic sign, the other sensors may be able to indicate that the sign recognized is incompatible with their inputs.

Thanks for Listening!

Questions?

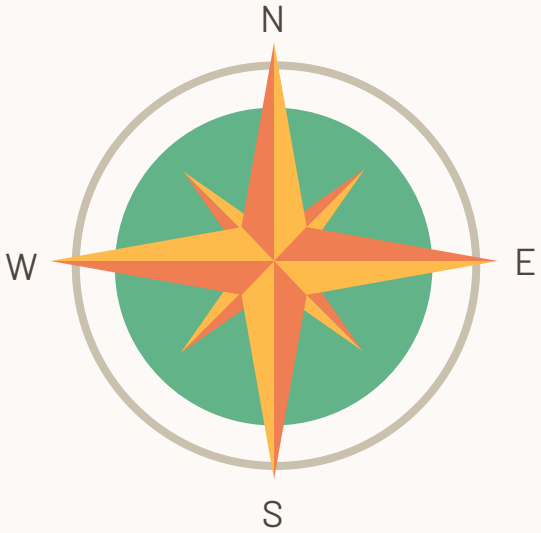
Discussion

Attack Implementation

How might an attacker implement any of the attacks discussed? (In-distribution, Out-of-Distribution, Lenticular Printing)

Potential Countermeasures

How might vehicle manufacturers or drivers defend against the proposed attacks?



Works Cited

Paper

- https://arxiv.org/pdf/1802.06430.pdf

Videos

- https://www.youtube.com/watch?v=DW23YmywLtU
- https://adversarial-learning.princeton.edu/darts/

CONTENTS OF THIS TEMPLATE

Here's what you'll find in this **Slidesgo** template:

1. A slide structure based on a multi-purpose presentation, which you can easily adapt to your needs. For more info on how to edit the template, please visit **Slidesgo School** or read our **FAQs**.
2. To view this template in PowerPoint with the correct fonts, download and install on your computer the **fonts that we have used**. You can learn how to download and install fonts **here.**
3. An assortment of graphic resources that are suitable for use in the presentation can be found in the **alternative resources** slide.
4. A **thanks** slide, which you must keep so that proper credits for our design are given.
5. A **resources** slide, where you'll find links to all the elements used in the template.
6. **Instructions for use**.
7. Final slides with:
    - The **fonts and colors** used in the template.
    - A selection of **illustrations**. You can also customize and animate them as you wish with the online editor. Visit **Storyset** to find more.
    - More **infographic resources**, whose size and color can be edited.
    - Sets of **customizable icons** of the following themes: general, business, avatar, creative process, education, help & support, medical, nature, performing arts, SEO & marketing, and teamwork.

You can delete this slide when you're done editing the presentation.

INTRODUCTION

You can give a brief description of the topic you want to talk about here. For example, if you want to talk about Mercury, you can say that it's the smallest planet in the entire Solar System

INTRODUCTION

You can give a brief description of the topic you want to talk about here. For example, if you want to talk about Mercury, you can say that it's the smallest planet in the entire Solar System

WHOA!

This can be the part of presentation where you can introduce yourself, write your email...

WHOA!

This can be the part of presentation where you introduce yourself, write your email...

WHOA!

This can be the part of presentation where you introduce yourself, write your email..

TABLE OF CONTENTS

TABLE OF CONTENTS

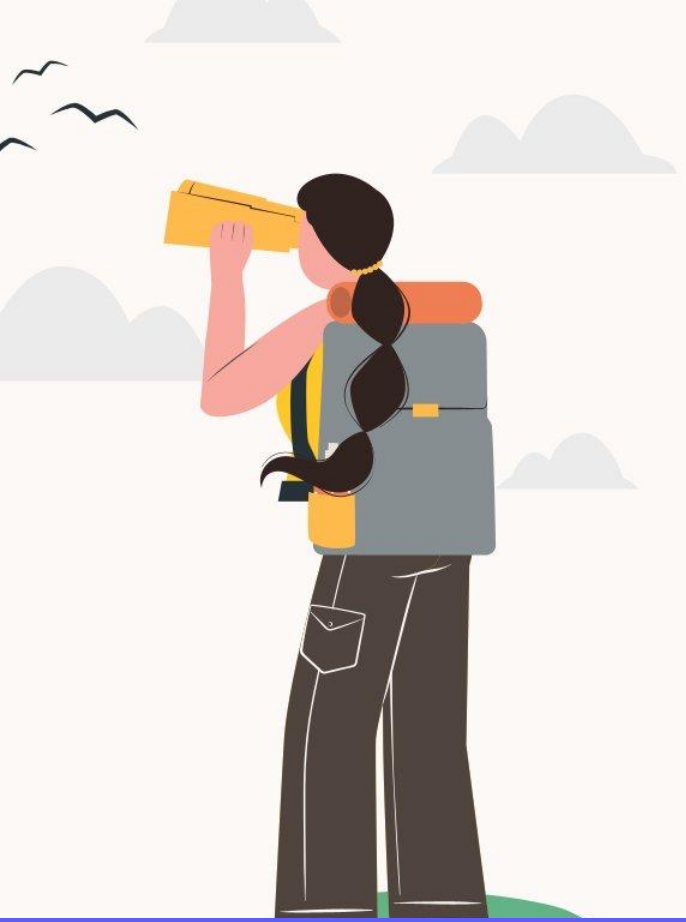
“This is a quote, words full of wisdom that someone important said and can make the reader get inspired.”

—SOMEONE FAMOUS

01

THE INDEX

You can enter a subtitle here if you need it



“This is a quote, words full of wisdom that someone important said and can make the reader get inspired.”

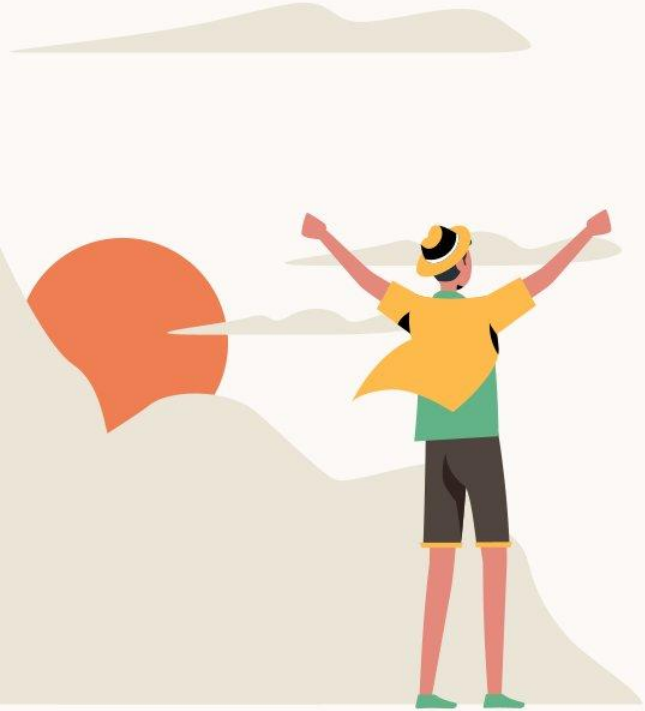
—SOMEONE FAMOUS

WOULD YOU BE ABLE TO READ A MAP OF THE ROAD?

Do you know what helps you make your point clear? Lists like this one:

- They’re simple
- You can organize your ideas clearly
- You’ll never forget to buy milk!

And the most important thing: the audience won’t miss the point of your presentation



WOULD YOU BE ABLE TO READ A MAP OF THE ROAD?

Do you know what helps you make your point clear? Lists like this one:

- They’re simple
- You can organize your ideas clearly
- You’ll never forget to buy milk!

And the most important thing: the audience won’t miss the point of your presentation

UNDERSTANDING THE INDEX

PLACES AND CITIES

Despite being red, Mars is actually a cold place. It’s full of iron oxide dust, which gives the planet its reddish cast

LABELS

Mercury is the closest planet to the Sun and the smallest one in the Solar System—it’s only a bit larger than the Moon

HOW TO USE THE INDEX?

SEARCH THE PLACE

Jupiter is a gas giant and the biggest planet in the Solar System

LOOK IN THE GRID

Saturn is the ringed planet. It's composed of hydrogen and helium

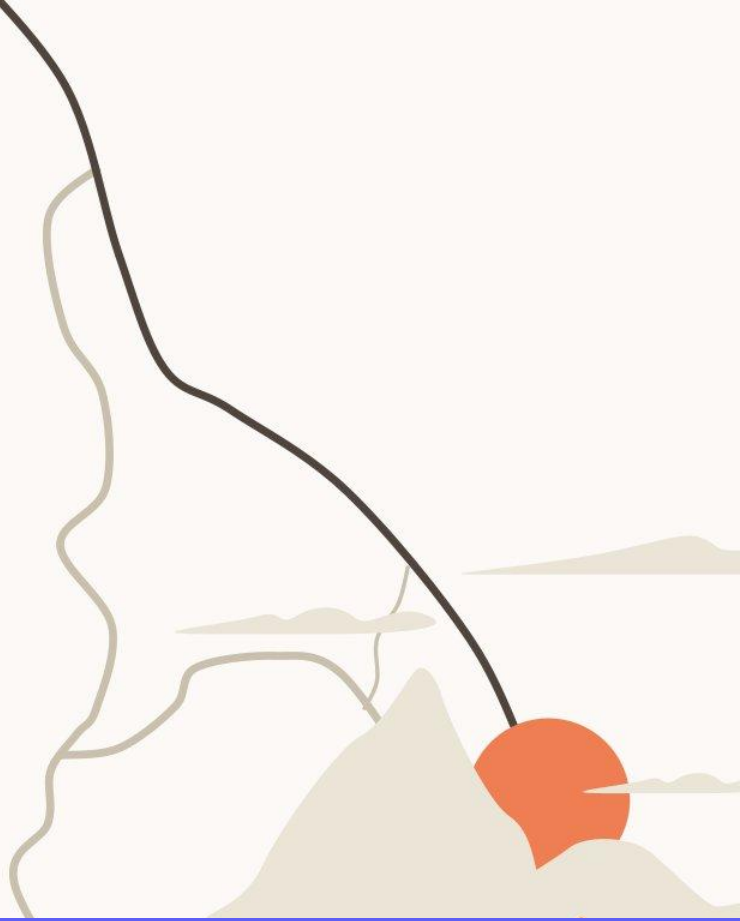
SEARCH IN THE ROW

Mercury is the closest planet to the Sun and the smallest one

02

THE LEGEND

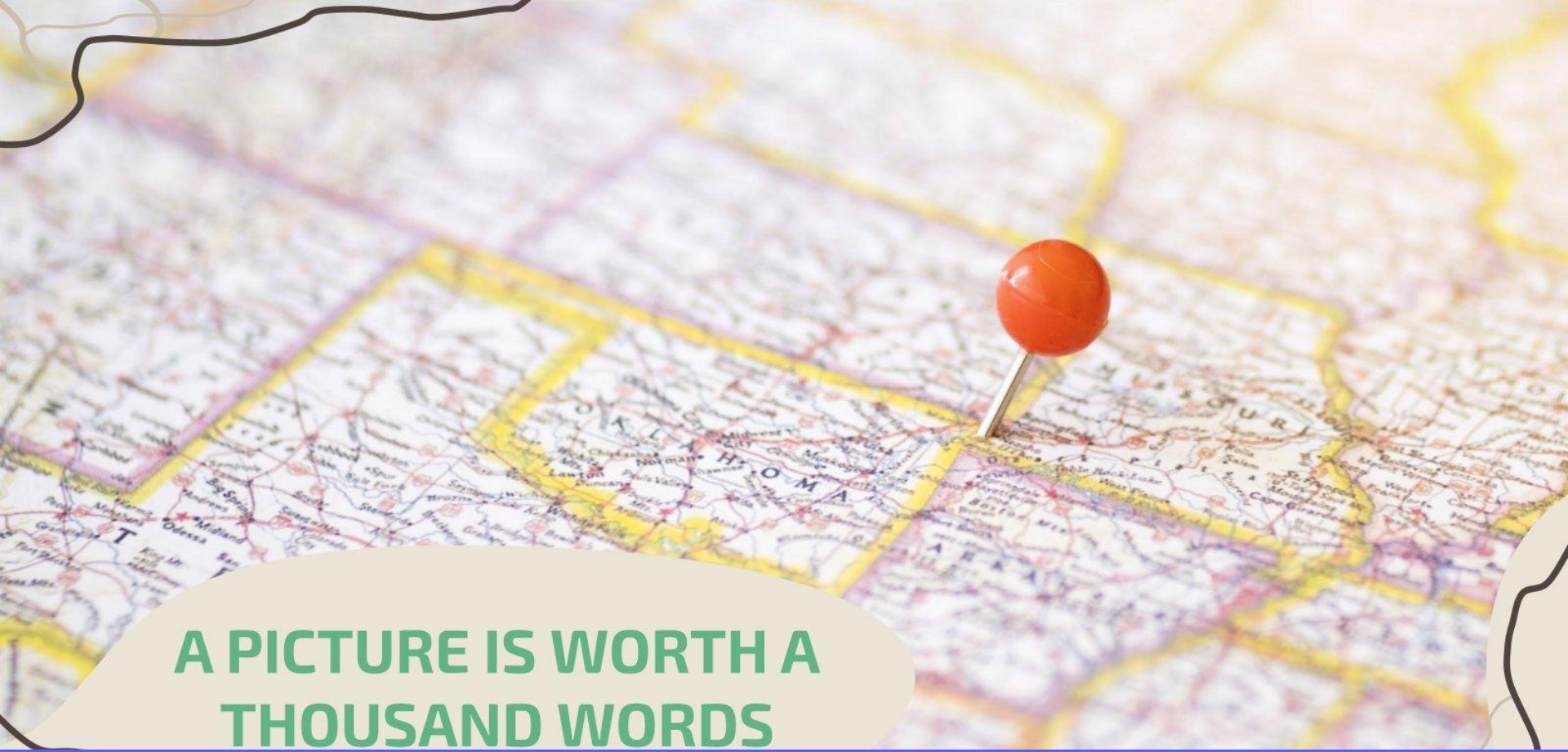
You can enter a subtitle here if you need it



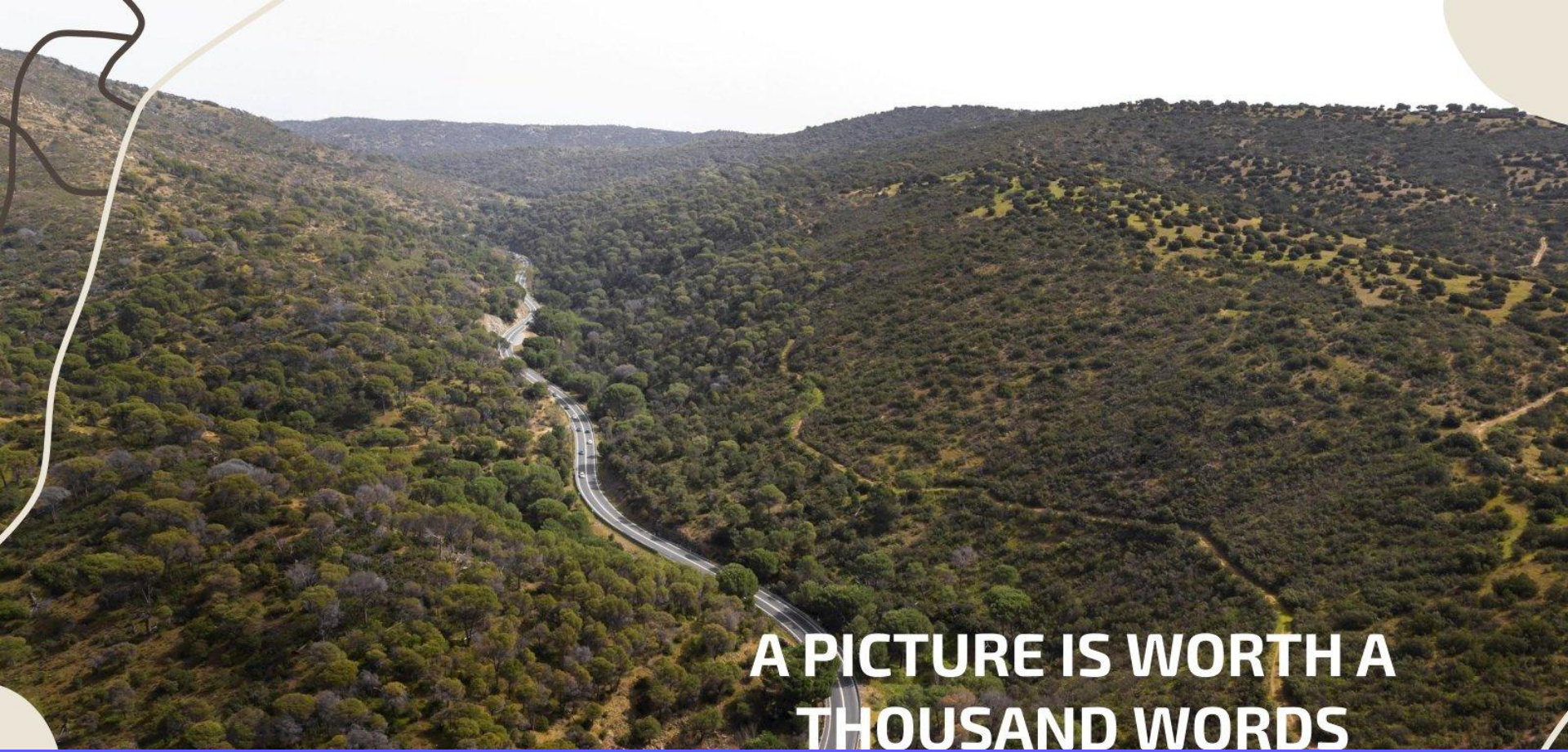
A PICTURE ALWAYS REINFORCES THE CONCEPTS

Images reveal large amounts of data, so remember: use an image instead of a long text. Your audience will appreciate it

A PICTURE IS WORTH A THOUSAND WORDS



A PICTURE IS WORTH A THOUSAND WORDS



AWESOME WORDS

Because key words are great for
catching your audience's attention

AWESOME WORDS

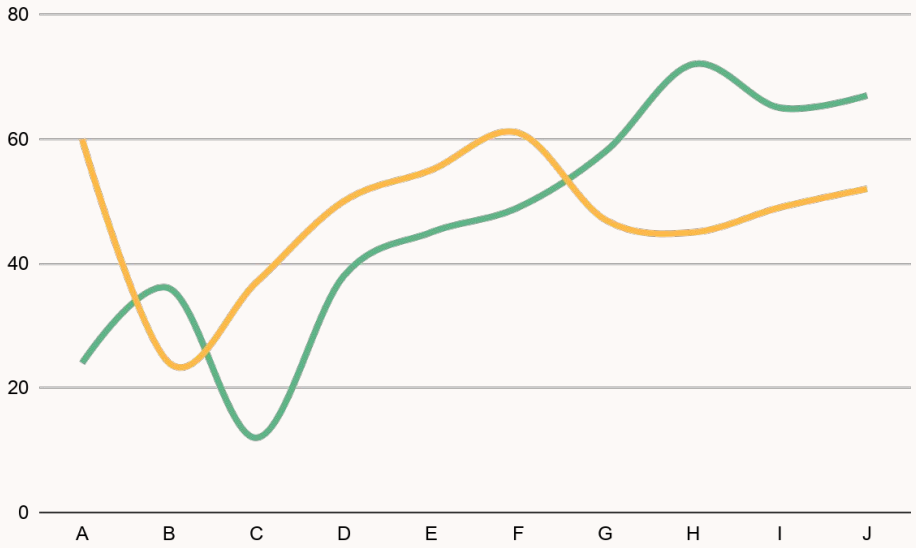
Because key words are great for catching your audience's attention

03

COMPASS ROSE

You can enter a subtitle here if you need it

THIS IS A GRAPH!



To modify this graph, click on it, follow the link, change the data and paste the new graph here

125,000

The Moon is a satellite

+190%

+175%

Jupiter is a gas giant and the biggest planet in the Solar System

REVIEWING CONCEPTS

NEPTUNE

Neptune is the farthest planet from the Sun

VENUS

Venus has a beautiful name, but it's terribly hot

JUPITER

Jupiter is the biggest planet in the Solar System

MARS

Despite being red, Mars is actually a cold place

THE MOON

The Moon is Earth's only natural satellite

SATURN

It's a gas giant. It's composed of hydrogen and helium

THIS IS A GRAPH!

MERCURY

It's the closest planet to the Sun

VENUS

Venus has a very toxic atmosphere

EARTH

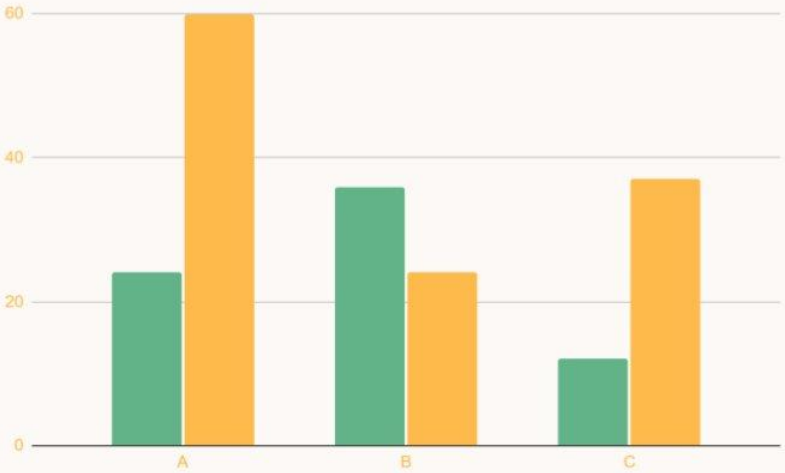
Earth is the planet where we all live

MARS

Mars is full of iron oxide dust

Follow the link in the graph to modify its data and then paste the new one here. **For more info, click here**

THIS IS ANOTHER GRAPH!



Follow the link in the graph to modify its data and then paste the new one here. **For more info, click here**

258,000

The Moon is a satellite

+76%

+133%

Jupiter is a gas giant and the biggest planet in the Solar System

04

TRIP PLANNING

You can enter a subtitle here if you need it

TOURISTIC MONUMENTS TO VISIT

MESA VERDE

The Moon is Earth's only natural satellite

MOUNT RUSHMORE

Venus has a beautiful name, but it's terribly hot

VENICE BEACH

Despite being red, Mars is

NAVY PIER

Jupiter is the biggest planet

RIVER WALK

Saturn is composed of

SOME ROAD TIPS

DRIVE SAFE

The Moon is Earth's only natural satellite

NO CELLPHONE

Venus has a beautiful name, but it's terribly hot

EYES ON THE ROAD

Jupiter is the biggest planet in the Solar System

TAKE A MAP

Saturn is a gas giant and has several rings

LISTEN TO MUSIC

Neptune is the farthest

SLEEP WELL

Despite being red, Mars is

INFOGRAPHIC

THE MAP

Neptune is the farthest planet from the Sun

COMPASS ROSE

Venus has a beautiful name, but it’s terribly hot

THE LANDMARKS

Jupiter is the biggest planet of them all

THE SCALE

Despite being red, Mars is a cold place

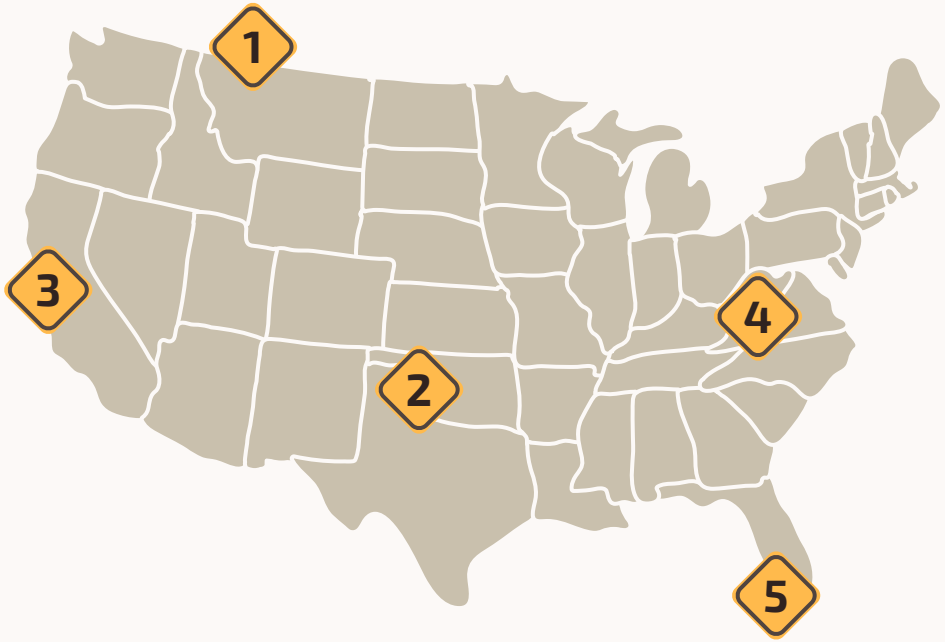
PLAN YOUR ROUTE!

ROUTE Going-to-the-Sun Road **DATE** April, 5

INDICATION	MILES	TIME	ATTRACTIONS
Saturn has several rings	7	45’	Jupiter, Venus
The moon is a satellite	13	1h24’	Earth, Saturn
Mars is a very cold place	27	2h12’	Mercury, The Moon
Jupiter is a gas giant	35	3h20’	Mars, Ceres, Vega

BEAUTIFUL US ROAD TRIPS

1. Going-to-the-Sun Road
2. Route 66
3. Highway 1 to Big Sur
4. Blue Ridge Parkway
5. Overseas Highway



TRIPS AROUND THE WORLD

1. Minnehaha Falls
2. Machu Picchu Ruins
3. Pyramids of Giza
4. New South Wales
5. New Delhi

THE SCALE

05

You can enter a subtitle here if you need it

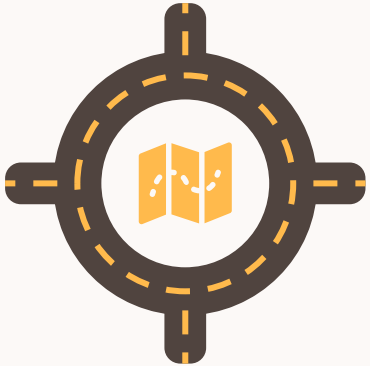
WHY LEARN TO READ A MAP?

VENUS

Venus has a beautiful name, but it's terribly hot

NEPTUNE

Neptune is the farthest planet from the Sun



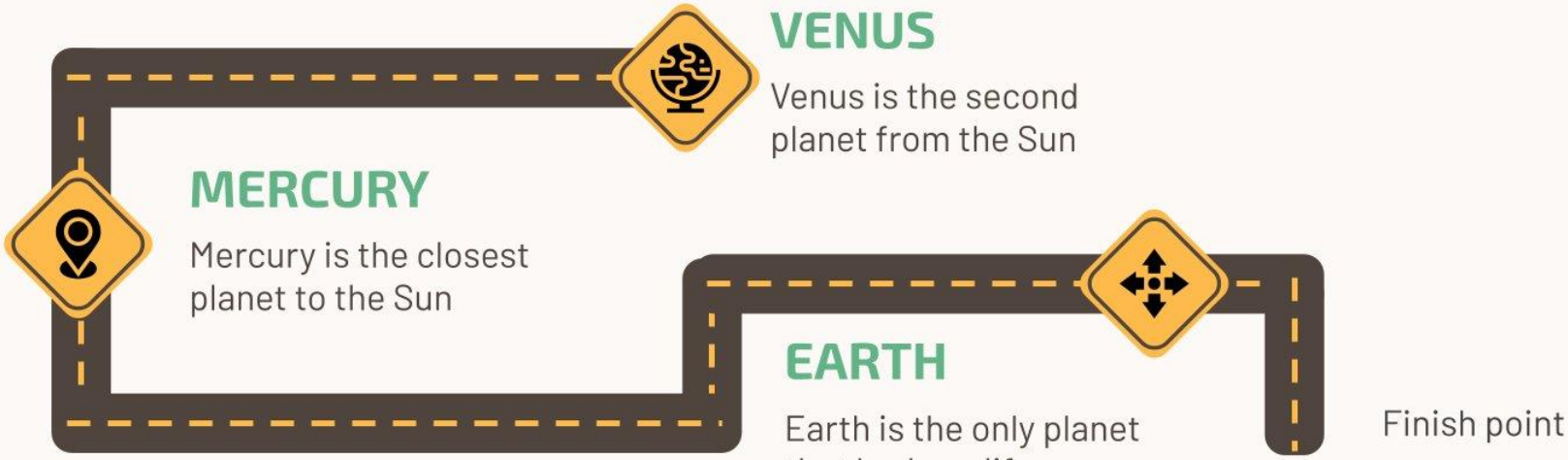
JUPITER

It's the biggest planet in the Solar System

MARS

Despite being red, Mars is a cold place

MINDSET NEEDED TO READ A MAP!



VENUS

Venus is the second planet from the Sun

MERCURY

Mercury is the closest planet to the Sun

EARTH

Earth is the only planet that harbors life

Finish point

INFORMATION NEEDED IN A MAP

MERCURY

Mercury is the closest planet to the Sun

JUPITER

Jupiter doesn't have a solid surface

VENUS

Venus is the second planet from the Sun

MARS

Despite being red, Mars is very cold

EARTH

Earth is the only planet that

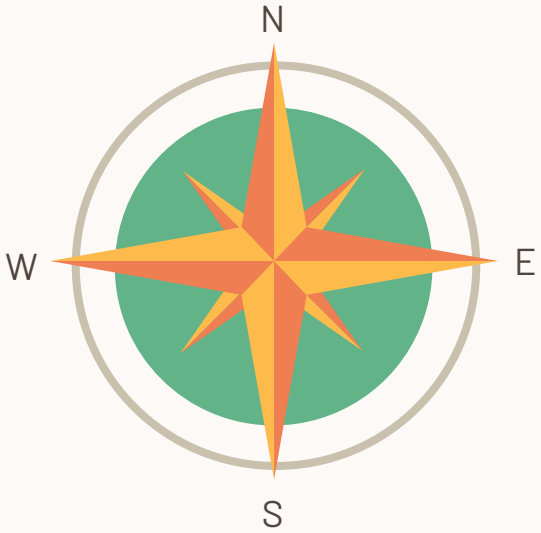
COMPASS ROSE

CARDINAL DIRECTIONS

Mercury is the closest planet to the Sun and also the smallest one in the Solar System

ORIENTATION

Despite being red, Mars is a very cold place. The planet is full of iron oxide dust



WHY STOP USING YOUR GPS?

JUPITER

Jupiter is the biggest planet in the Solar System

NEPTUNE

Neptune is the farthest planet from the Sun

VENUS

Venus has a beautiful name, but it's terribly hot

HOW TO READ SOME SIGNS?

MERCURY

Mercury is the closest planet to the Sun

EARTH

Venus is the second planet from the Sun

VENUS

Earth is the only planet that harbors life

MARS

Despite being red, Mars is actually a cold place

BIKEPACKING? WHY NOT?

NEPTUNE

It's the farthest planet from the Sun

VENUS

It has a beautiful name, but it's very hot

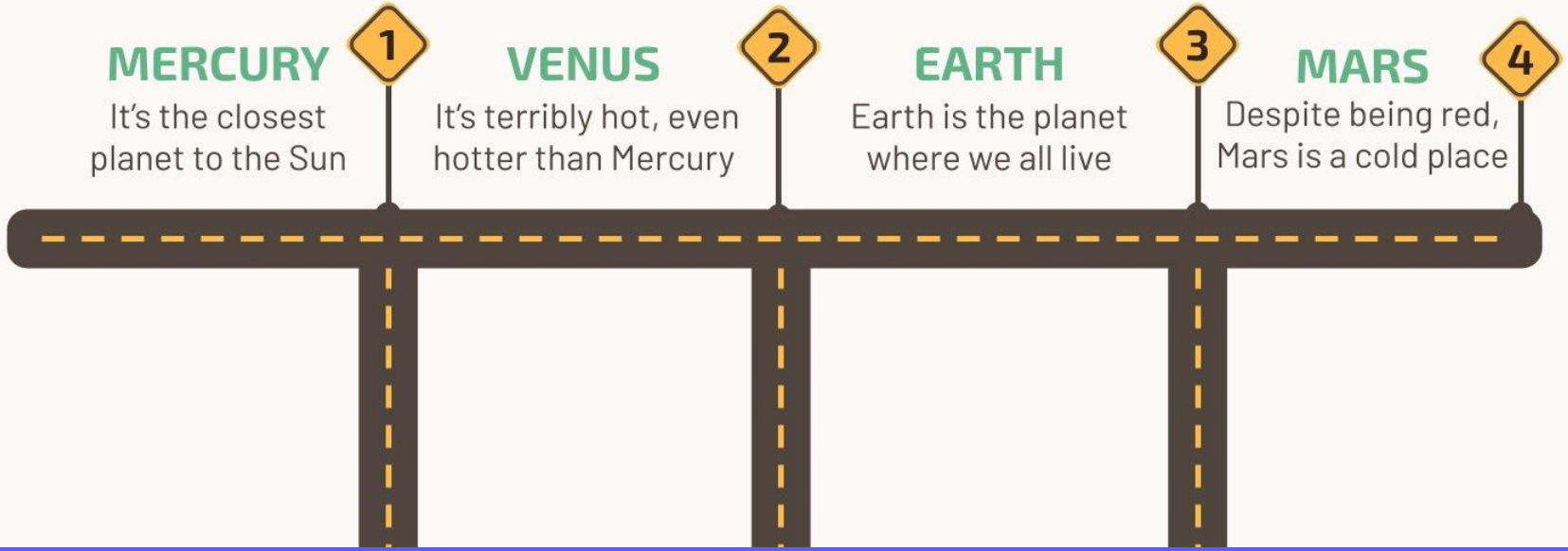
MERCURY

Mercury is the closest planet to the Sun

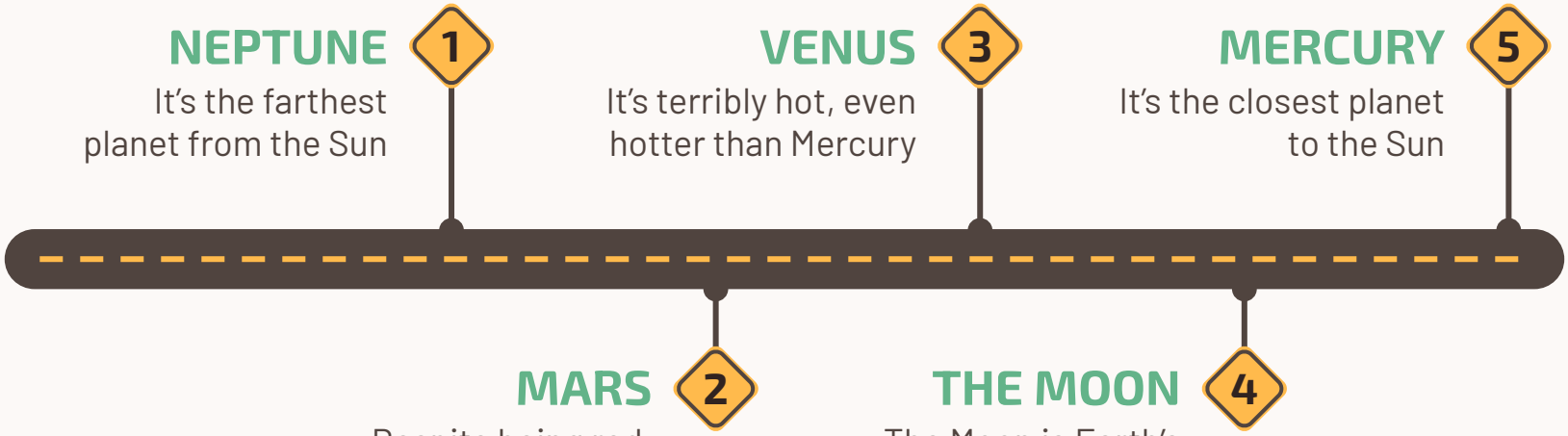
JUPITER

It's the biggest planet in the Solar System

TIMELINE



TIMELINE


NEPTUNE
1
It's the farthest planet from the Sun
MARS
2
Despite being red, Mars is a cold place
VENUS
3
It's terribly hot, even hotter than Mercury
THE MOON
4
The Moon is Earth's only natural satellite
MERCURY
5
It's the closest planet to the Sun

3,995,644

miles of roads in the United States

TELL ME THE CARDINALS!

NORTH

Despite being red, Mars is a cold place

EAST

Mercury is the smallest planet

WEST

Earth is the planet where we all live

SOUTH

Venus has a

333,000

The Sun’s mass compared to Earth’s

9H 55M 23S

Jupiter’s rotation period

386,000 km

Distance between Earth and the Moon

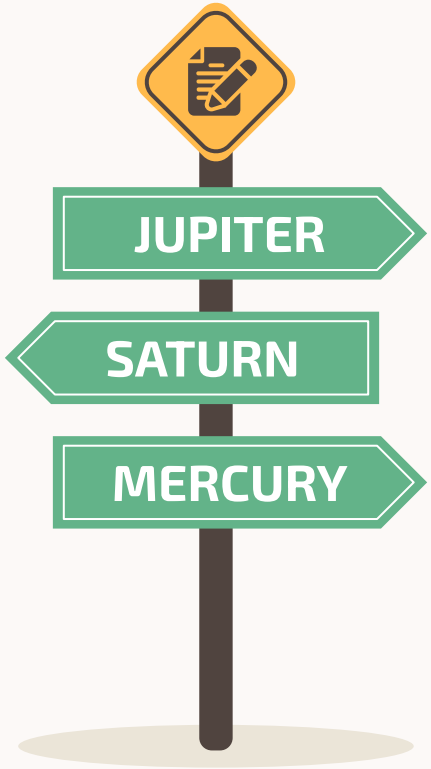
PROBABLY, THE MOST FAMOUS ROUTE

THE ROUTE 66

Despite being red, Mars is a cold place. It's full of iron oxide dust, which gives the planet its reddish cast!

Earth is the third planet from the Sun and the only planet known to harbor life!

SOME TIPS FOR YOUR TRIP!



THE MAP

Neptune is the farthest planet from the Sun

THE SPEED

Jupiter is the biggest planet of them all

THE SCALE

Despite being red, Mars is a cold place

SOME PERCENTAGES!

MARS

Despite being red, Mars is actually a very cold place. It's full of iron oxide dust

MERCURY

Mercury is the closest planet to the Sun and the smallest one

VENUS

Venus is the second planet from the Sun. It's really hot there

SOME INTERESTING PLACES

NEPTUNE

It's the farthest planet from the Sun

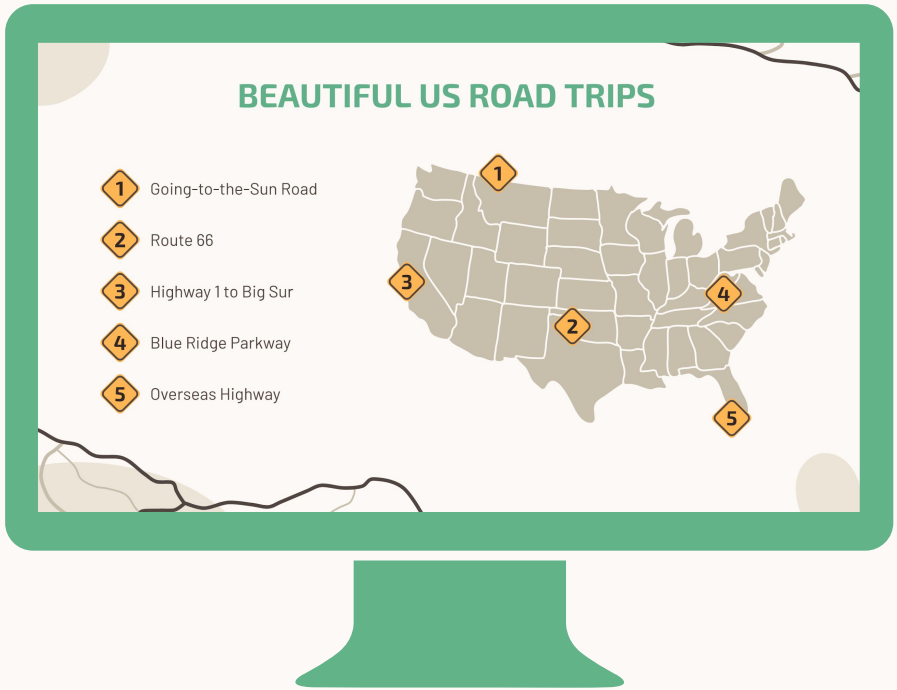
VENUS

It's terribly hot, even hotter than Mercury

MARS

Despite being red, Mars is a cold place

DESKTOP MOCKUP



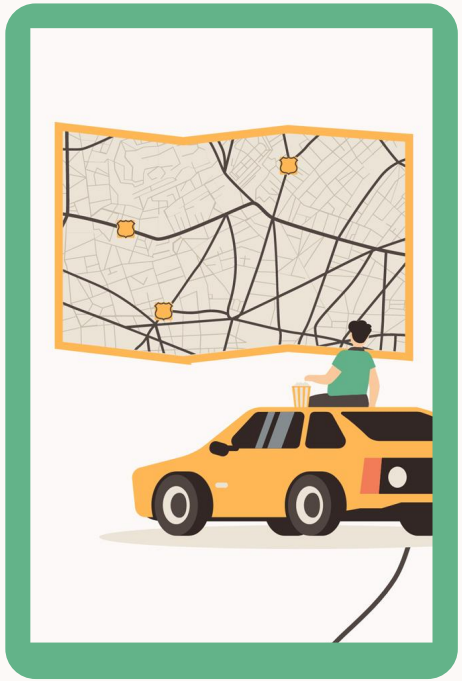
You can replace the image on the screen with your own work. Right click on it and choose "Replace image" so you can add yours

LAPTOP MOCKUP

You can replace the image on the screen with your own work. Right click on it and choose "Replace image" so you can add yours

TABLET MOCKUP

You can replace the image on the screen with your own work. Right click on it and choose "Replace image" so you can add yours



WRITE A WORD FOR EACH PLACE!

PLACE	CATCHWORD
Mount Rushmore	Mercury
Mississippi River	Venus
Central Park	Earth
Grand Canyon	Mars

DO'S AND DON'TS

Mercury is the closest planet to the Sun

Despite being red, Mars is actually a cold place

Venus is the second planet from the Sun

Jupiter is the biggest planet of them all

Earth is the only planet that harbors life

Saturn is a gas giant and has several rings

PHONE MOCKUP

You can replace the image on the screen with your own work. Right click on it and choose "Replace image" so you can add yours

MEDIA

"Despite being red, Mars is a cold place. The planet is full of iron oxide dust"

—TRAVEL MAGAZINE

"Saturn is the ringed planet. It's composed mostly of hydrogen and helium"

—ON THE ROAD

"Neptune is the farthest planet from the Sun. It's a really cold place"

—ON YOUR WHEELS

"Venus has a beautiful name and is the second planet from the Sun"

—ROADS THE WORLD

OUR TEAM

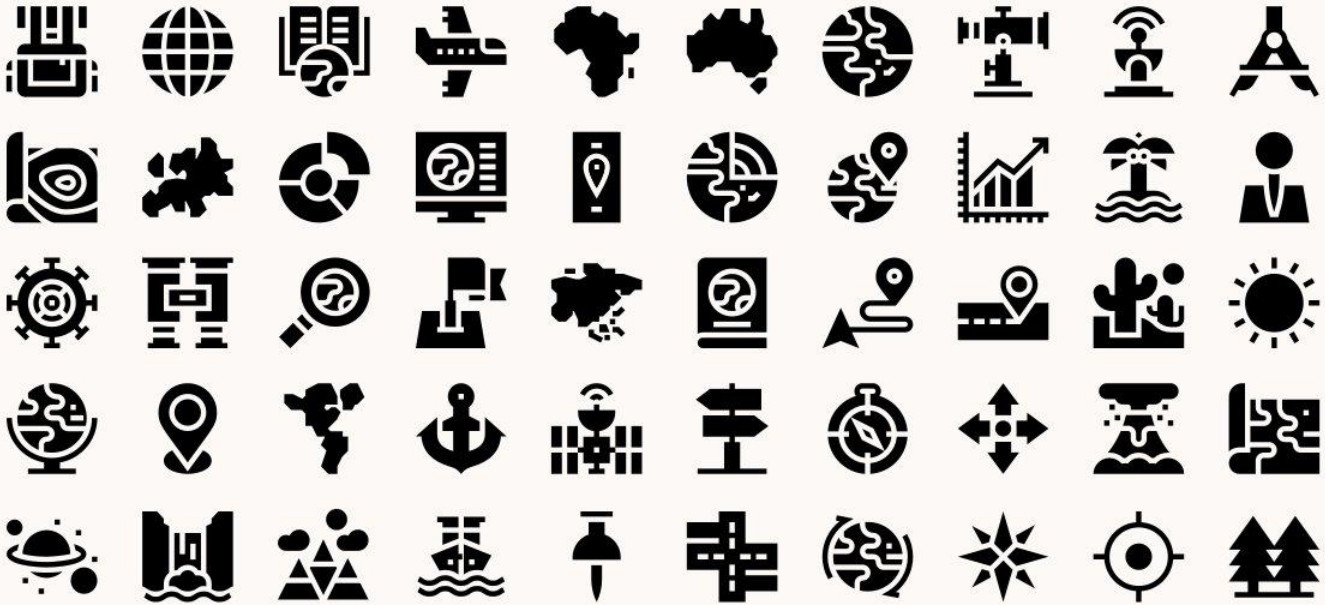
LAURA MILLER

You can talk a bit about this person here. Replace the image if needed

ANDY WILSON

You can talk a bit about this person here. Replace the image if needed

ICON PACK



THANKS!

Do you have any questions?

addyouremail@freepik.com
+91 620 421 838
yourcompany.com

ALTERNATIVE RESOURCES

Here's an assortment of alternative resources whose style fits that of this template

- Flat map compass collection

ALTERNATIVE RESOURCES

MERCURY

It's the closest planet to the Sun

VENUS

It's terribly hot, even hotter than Mercury

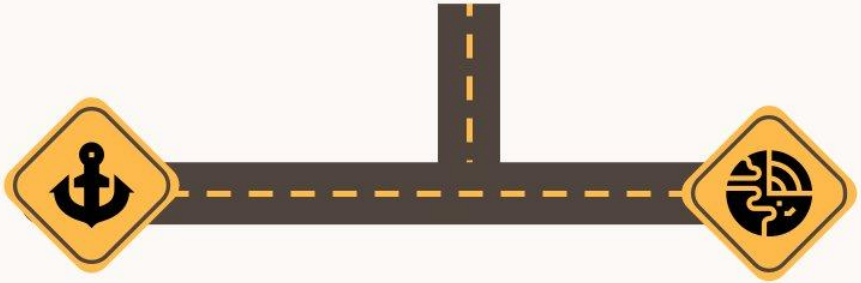
MIND MAP

EARTH

Earth is the planet where we all live

MARS

Despite being red, Mars is a cold place



ALTERNATIVE RESOURCES

PREMIUM RESOURCES

PHOTOS

- Defocused complex map with pinpoint
- Transport concept with road and nature
- Defocused complex map with pinpoint

ICONS

- Icon Pack: Geography | Filled

STORYSET

- Off Road
- Lost
- Exploring

RESOURCES

VECTORS

- Black and white town navigation on map
- Colorful compasses pack
- Informational city map with streets name
- Route 66 road sign

PHOTOS

- Desert landscape
- Close-up of female friends sitting in the car looking at map
- Pretty young woman enjoying road trip
- Smiling young african american man standing near car on beach

STORYSET

- By my car
- Drive-in movie theater
- Paper map
- Directions
- Exploring
- Toronto
- World
- Vehicle Sale

ICONS

- Building
- Motorcycle
- Sports car

Instructions for use

If you have a free account, in order to use this template, you must credit **Slidesgo** by keeping the **Thanks** slide. Please refer to the next slide to read the instructions for premium users.

As a Free user, you are allowed to:

- Modify this template.
- Use it for both personal and commercial projects.

You are not allowed to:

- Sublicense, sell or rent any of Slidesgo Content (or a modified version of Slidesgo Content).
- Distribute Slidesgo Content unless it has been expressly authorized by Slidesgo.
- Include Slidesgo Content in an online or offline database or file.
- Offer Slidesgo templates (or modified versions of Slidesgo templates) for download.
- Acquire the copyright of Slidesgo Content.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

https://slidesgo.com/faqs and https://slidesgo.com/slidesgo-school

Instructions for use (premium users)

As a Premium user, you can use this template without attributing **Slidesgo** or keeping the "**Thanks**" slide.

You are allowed to:

- Modify this template.
- Use it for both personal and commercial purposes.
- Hide or delete the “Thanks” slide and the mention to Slidesgo in the credits.
- Share this template in an editable format with people who are not part of your team.

You are not allowed to:

- Sublicense, sell or rent this Slidesgo Template (or a modified version of this Slidesgo Template).
- Distribute this Slidesgo Template (or a modified version of this Slidesgo Template) or include it in a database or in any other product or service that offers downloadable images, icons or presentations that may be subject to distribution or resale.
- Use any of the elements that are part of this Slidesgo Template in an isolated and separated way from this Template.
- Register any of the elements that are part of this template as a trademark or logo, or register it as a work in an intellectual property registry or similar.

For more information about editing slides, please read our FAQs or visit Slidesgo School:

https://slidesgo.com/faqs and https://slidesgo.com/slidesgo-school

Fonts & colors used

This presentation has been made using the following fonts:

Exo 2
(https://fonts.google.com/specimen/Exo+2)

Barlow
(https://fonts.google.com/specimen/Barlow)

Storyset

Create your Story with our illustrated concepts. Choose the style you like the most, edit its colors, pick the background and layers you want to show and bring them to life with the animator panel! It will boost your presentation. Check out how it works.

Pana

Amico

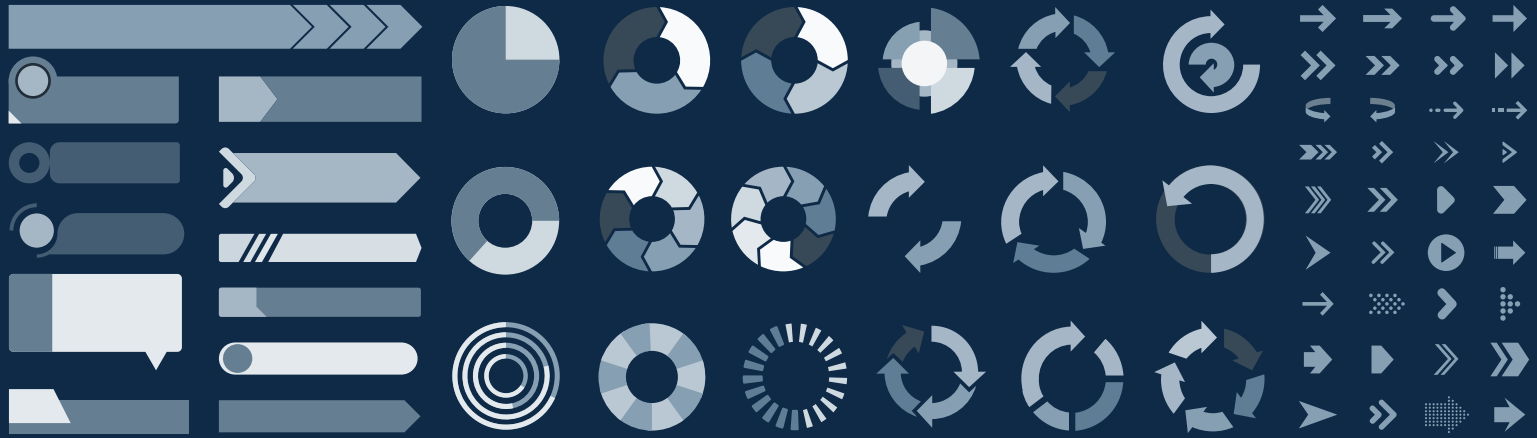
Bro

Rafiki

Cuate

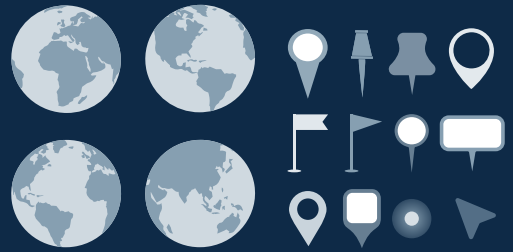
Use our editable graphic resources...

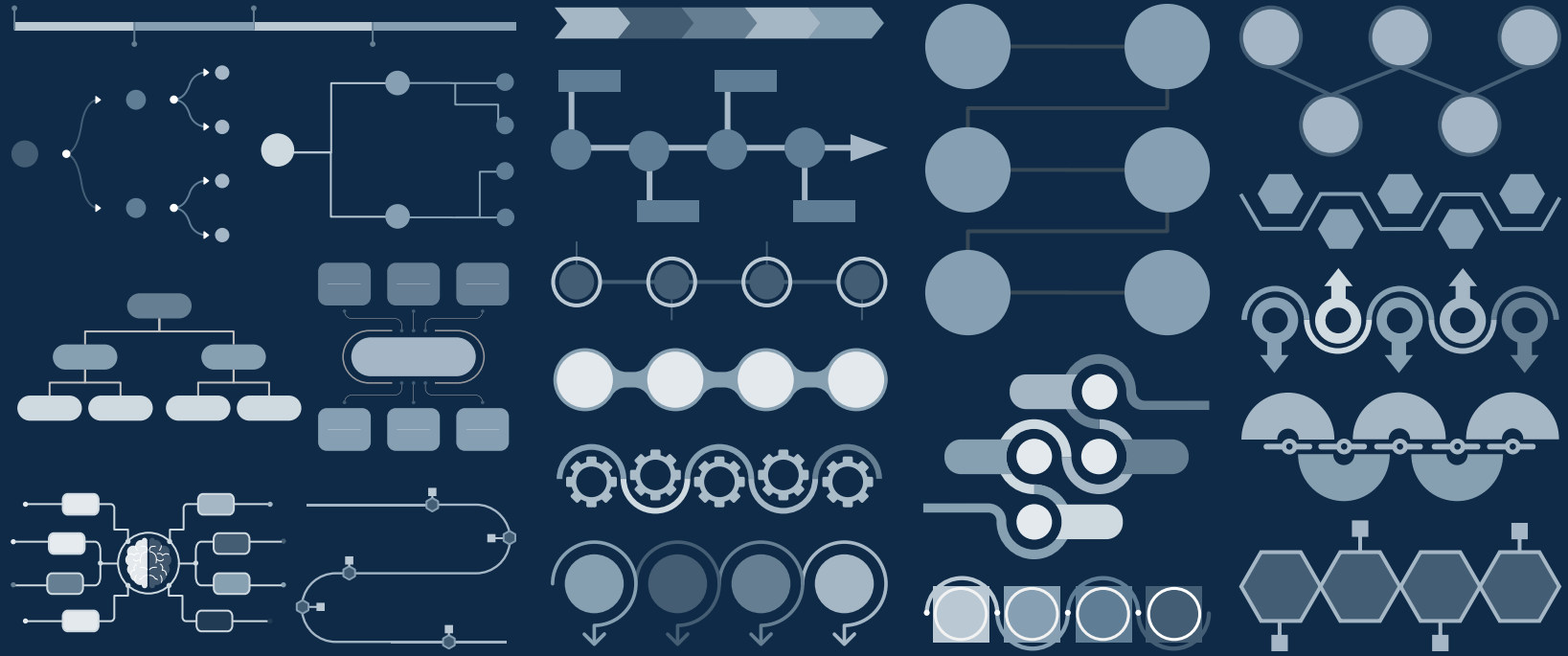
You can easily resize these resources without losing quality. To change the color, just ungroup the resource and click on the object you want to change. Then, click on the paint bucket and select the color you want. Group the resource again when you're done. You can also look for more infographics on Slidesgo.

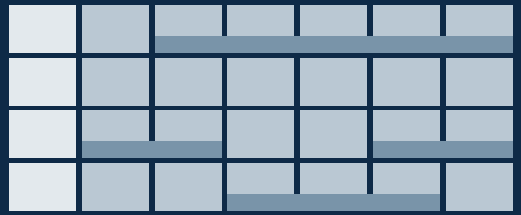


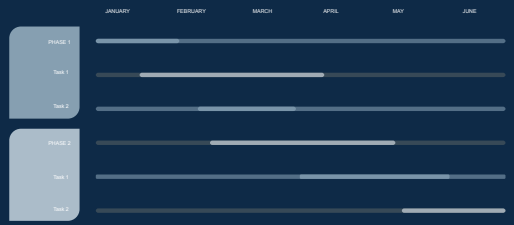


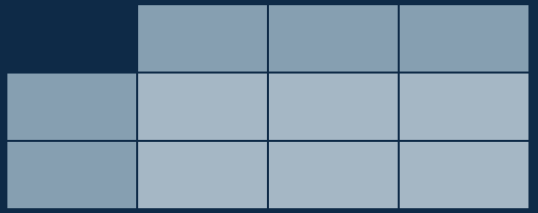


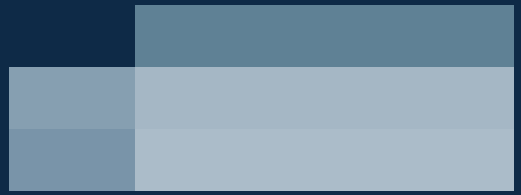



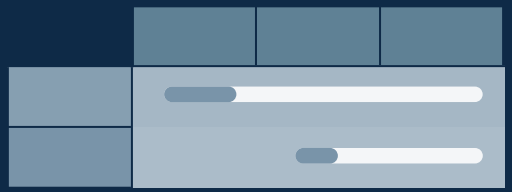


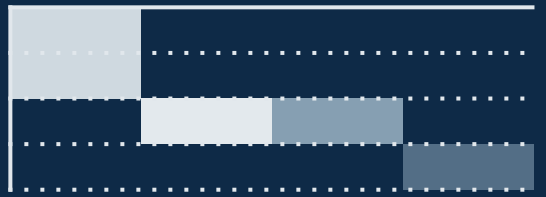


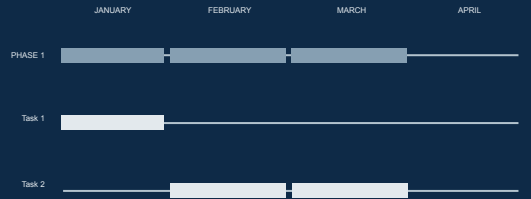

JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
PHASE 1
Task 1
Task 2
PHASE 2
Task 1
Task 2

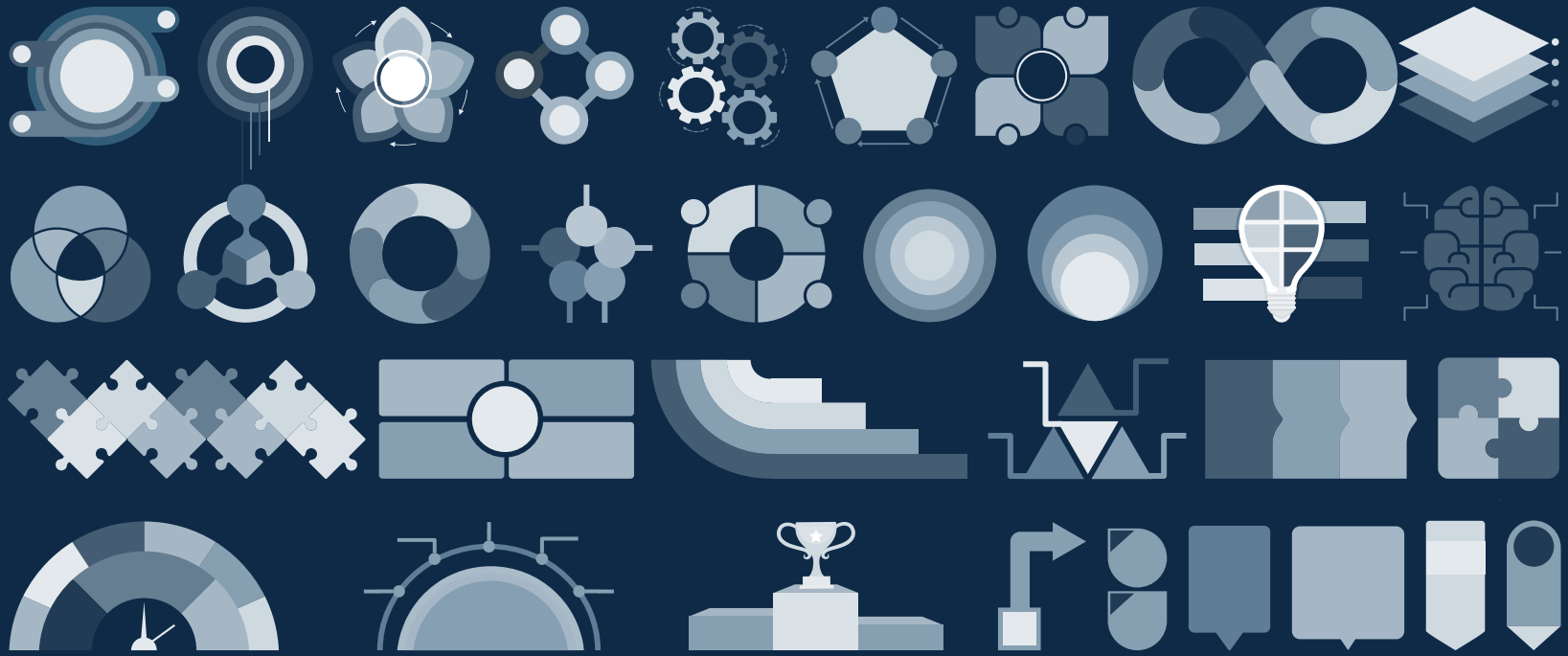









JANUARY
FEBRUARY
MARCH
APRIL
PHASE 1
Task 1
Task 2



...and our sets of editable icons

You can resize these icons without losing quality.
You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.
In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.

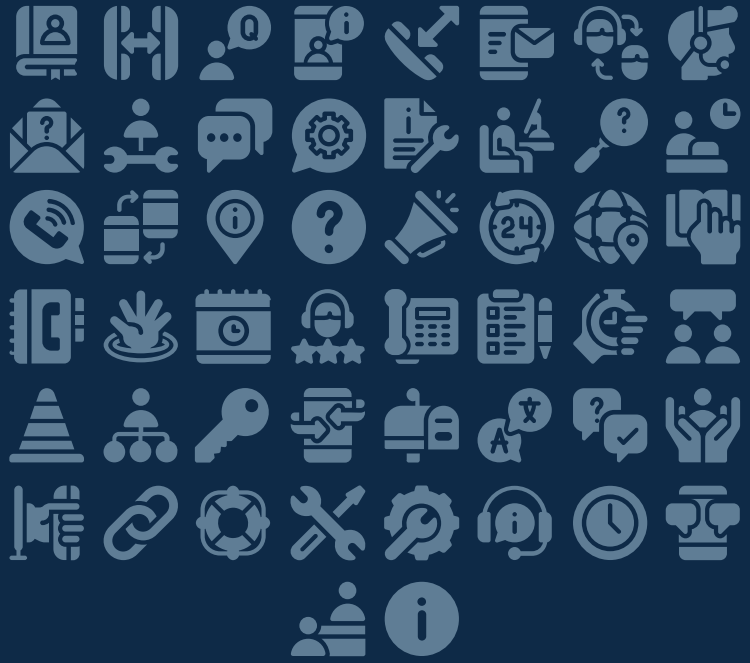
Educational Icons

Medical Icons

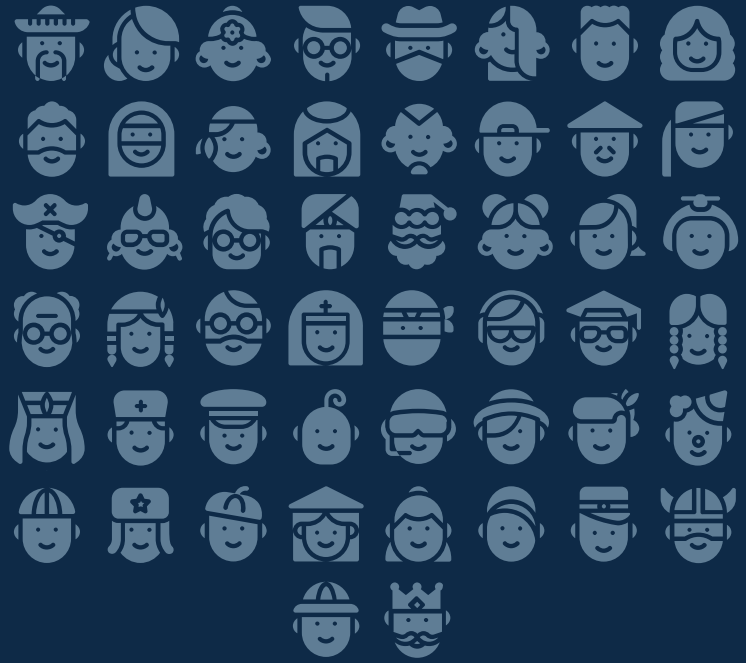
Business Icons

Teamwork Icons

Help & Support Icons



Avatar Icons



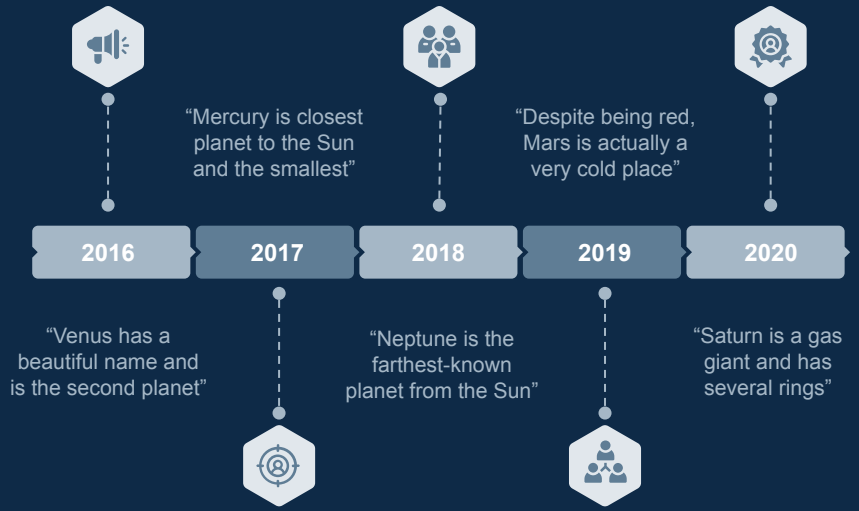
Creative Process Icons

Performing Arts Icons

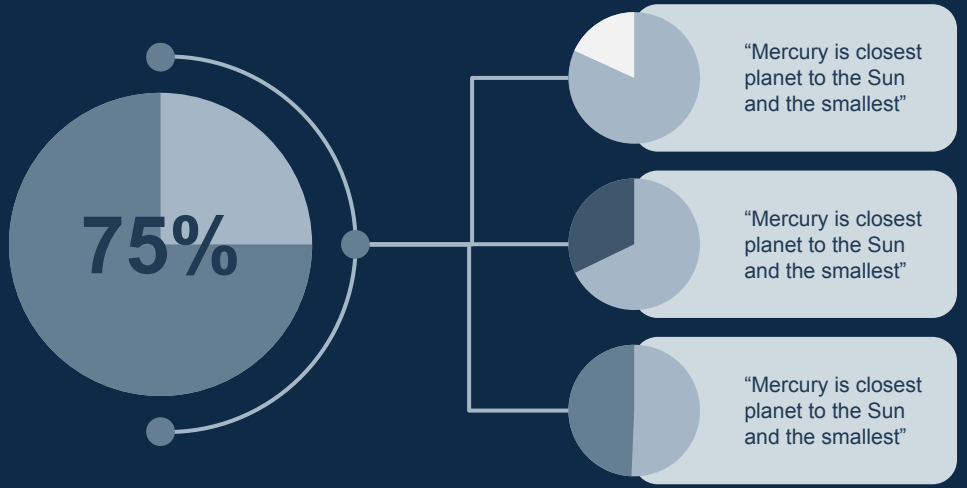
Nature Icons

SEO & Marketing Icons

Premium infographics

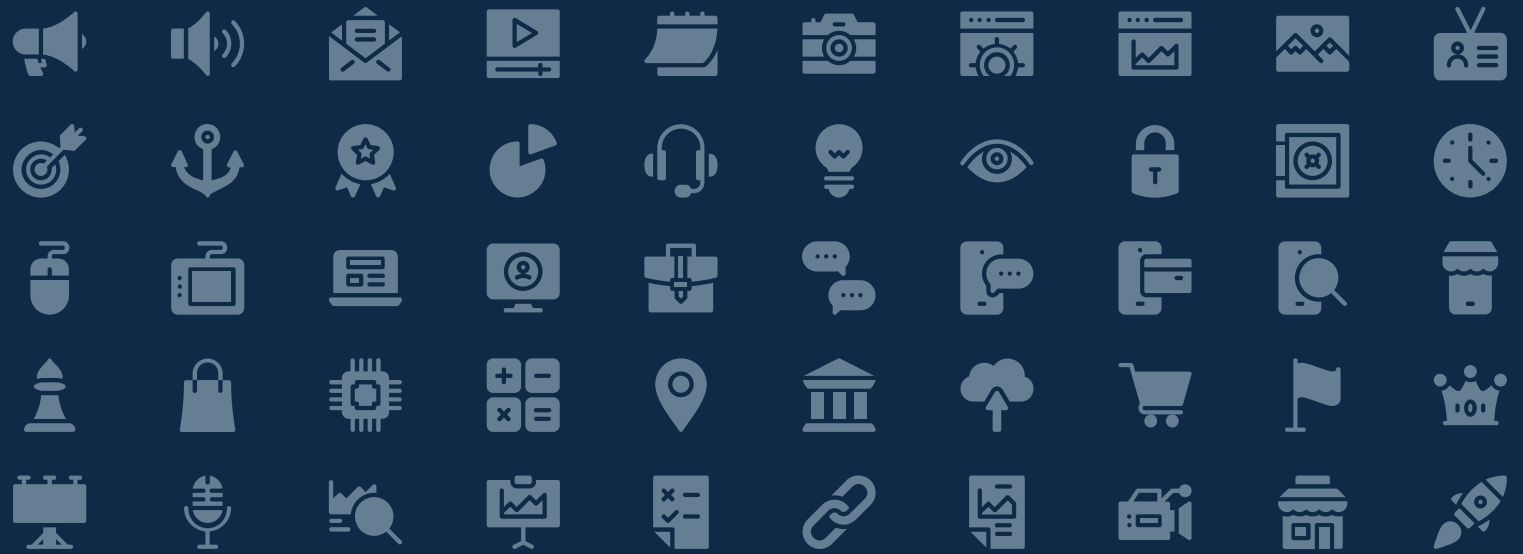


Premium infographics



Premium Icons

Digital Marketing



Premium Icons

Online Learning

Premium Icons

Laboratory

Premium Icons

Goals & Results

Premium Icons

Infographic Elements


slidesgo