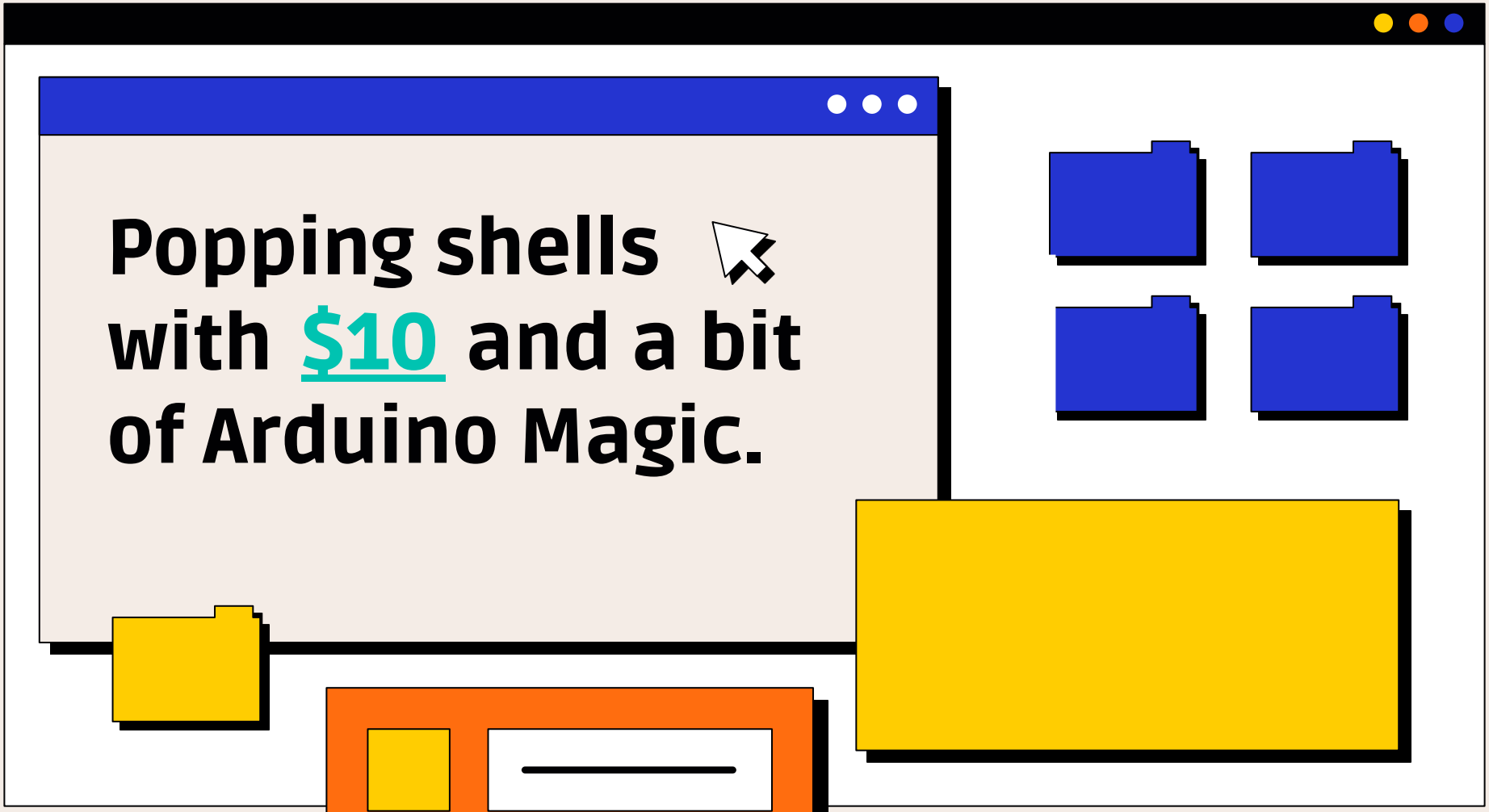
Popping shells with $10 and a bit of Arduino Magic.



Let’s Redefine

Physical Access



Table of contents

01

About

Who am I?
What is this?

02

The Phrase

“That would require extended physical access”

03

A New Definition

How far away can that really be?

04

More Info

Links, info, etc

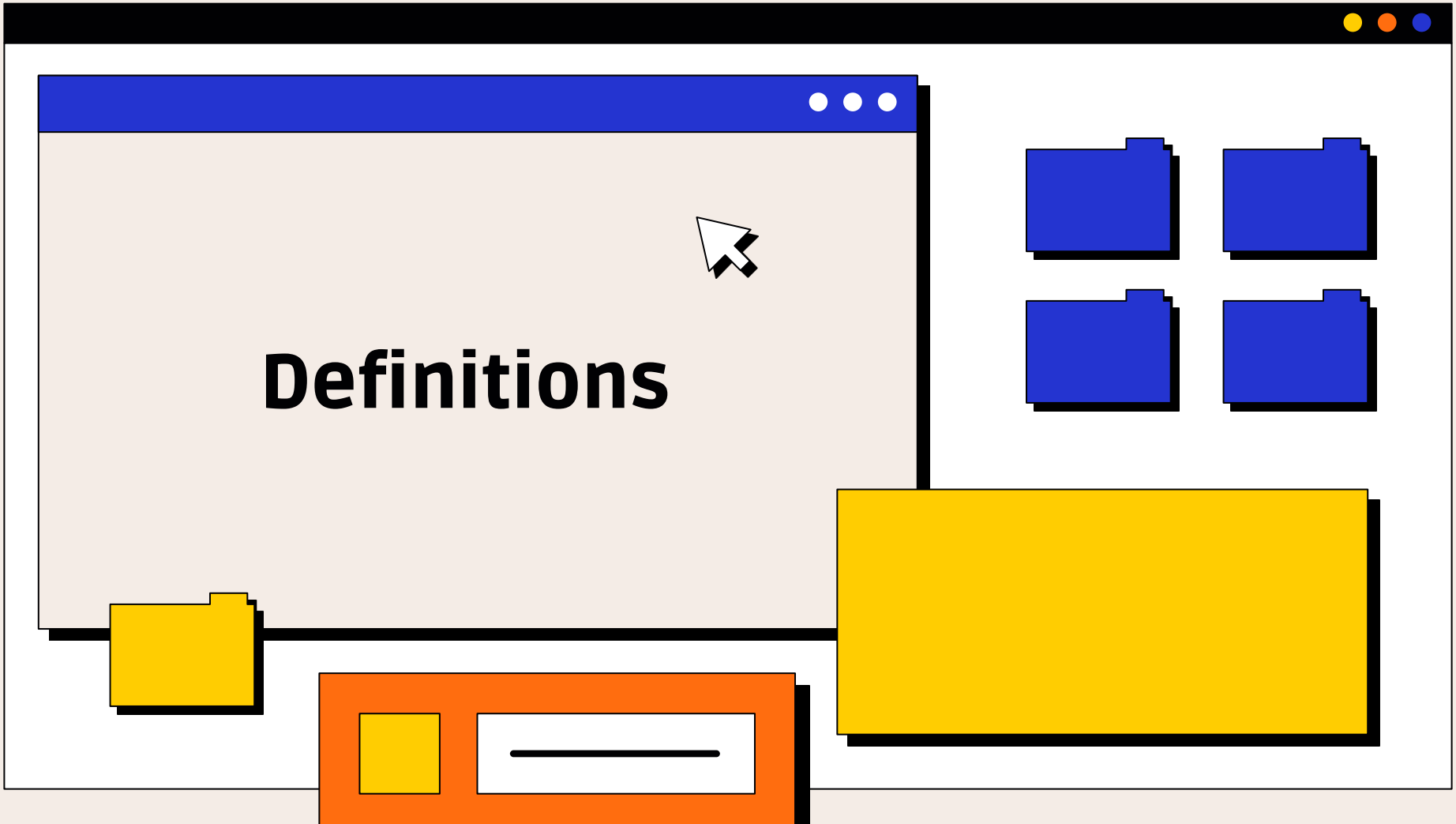
Who am I?

- Software Engineer at Medcrypt
- Director of MedISAO
- Previously CTO of Promenade Software
    - Worked on 10+ medical devices. Collaborated on even more. Designed and Implemented
        - **IVD instruments**
        - Implantables
        - **Therapeutic Devices**
        - Infusion Pumps
        - You name it

All views expressed are my own and do not reflect the opinions of my current or past employers



Definitions

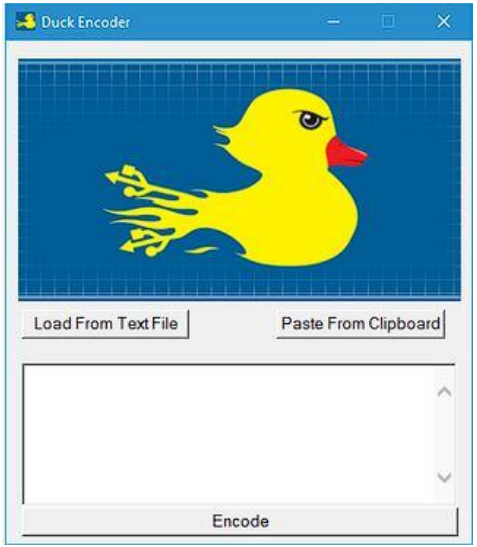


What is a BadUSB?

USB dongle announces itself as a HID Device.

It can lie and say that it’s a mouse, keyboard, ethernet, etc

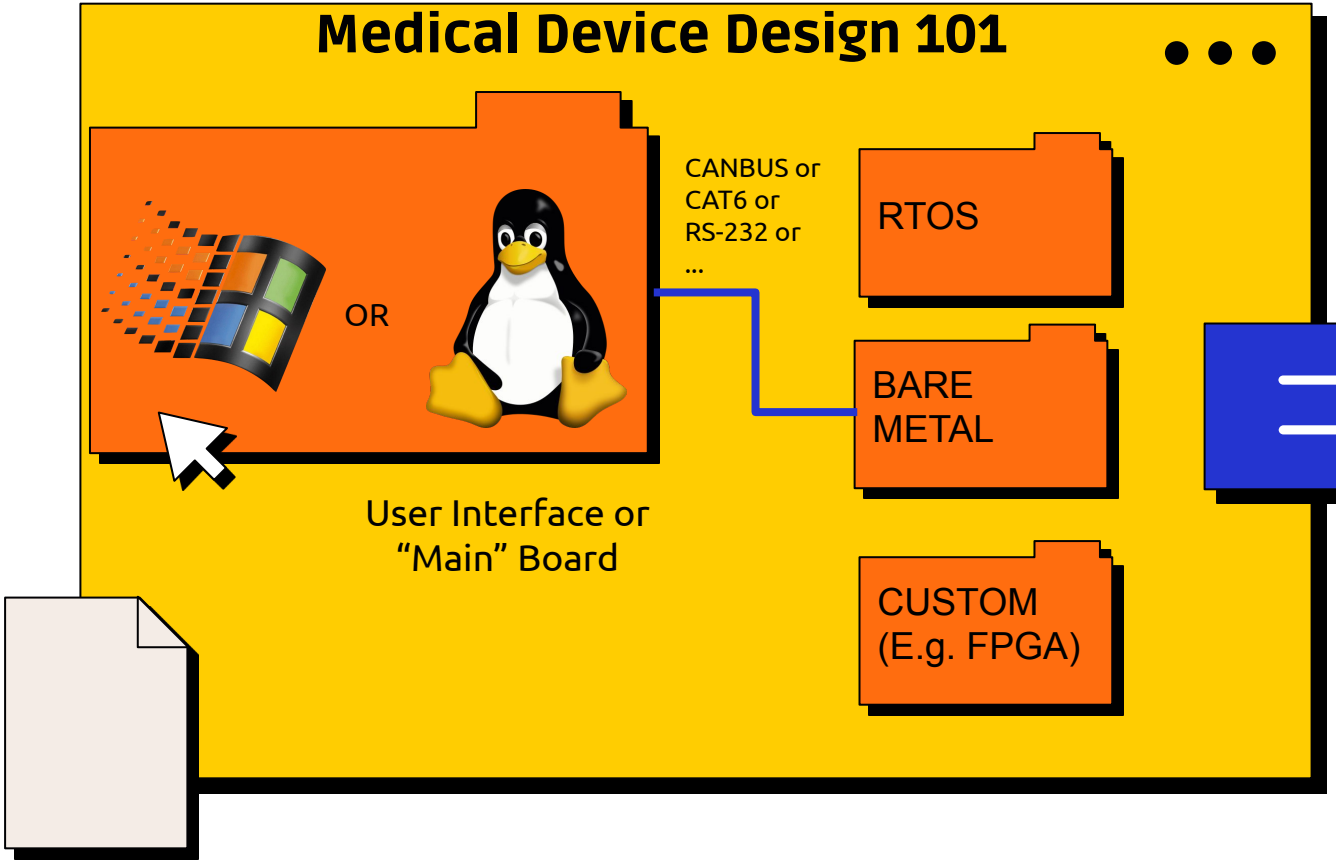


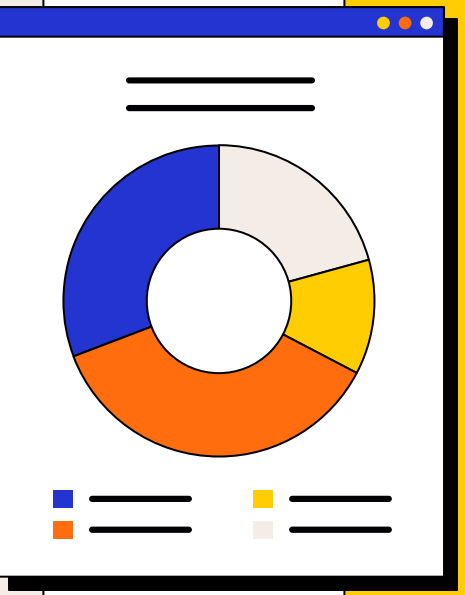

Duck Encoder
Load From Text File
Paste From Clipboard
Encode

Examples




O.MG ELITE

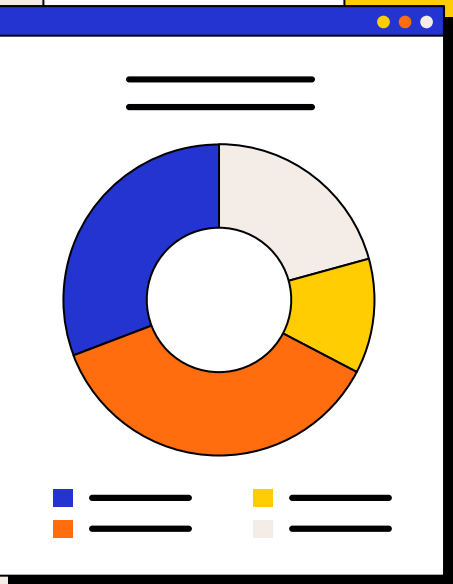

Medical Device Design 101
OR
CANBUS or
CAT6 or
RS-232 or
...
RTOS
BARE
METAL
CUSTOM
(E.g. FPGA)
User Interface or
“Main” Board



BadUSB?
In my med device?
It's not that bad

To exploit it would require:

- Physical access for an extended period of time. or
- An internet connection for persistence



BadUSB?
In my med device?

It's more likely than you think

To exploit it would require:

- Physical access for ~~an extended~~ a short period of time.
- ~~An internet connection for persistence~~ We can bring our OWN internet connection



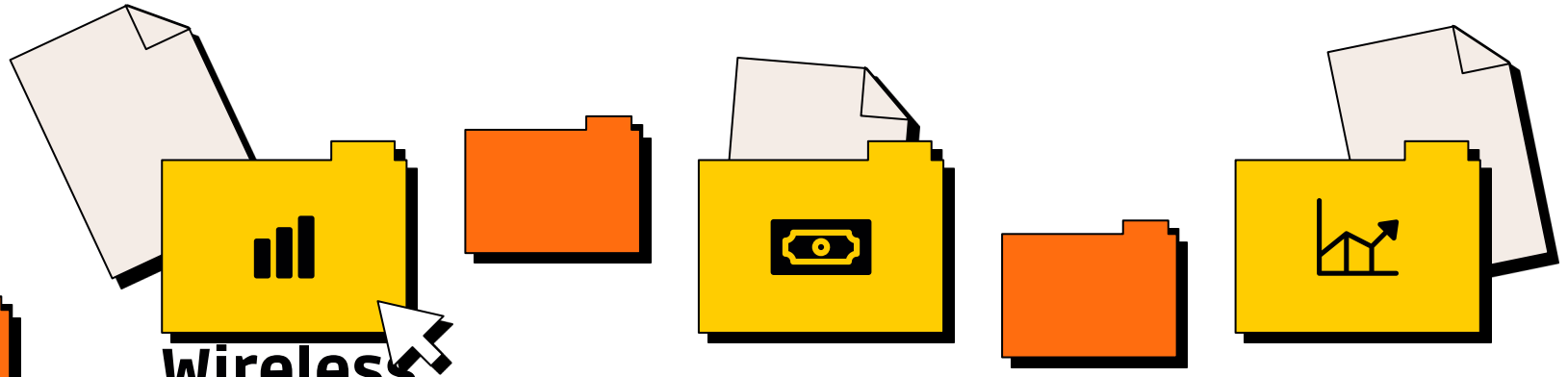








What do we need?



Wireless Control

Long distance wireless communication onboard the implant.

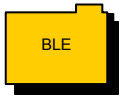
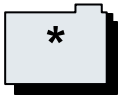
Cheap

We don’t want to worry about retrieving them

USB Emulation

We need USB HID to actually do the BadUSB dance

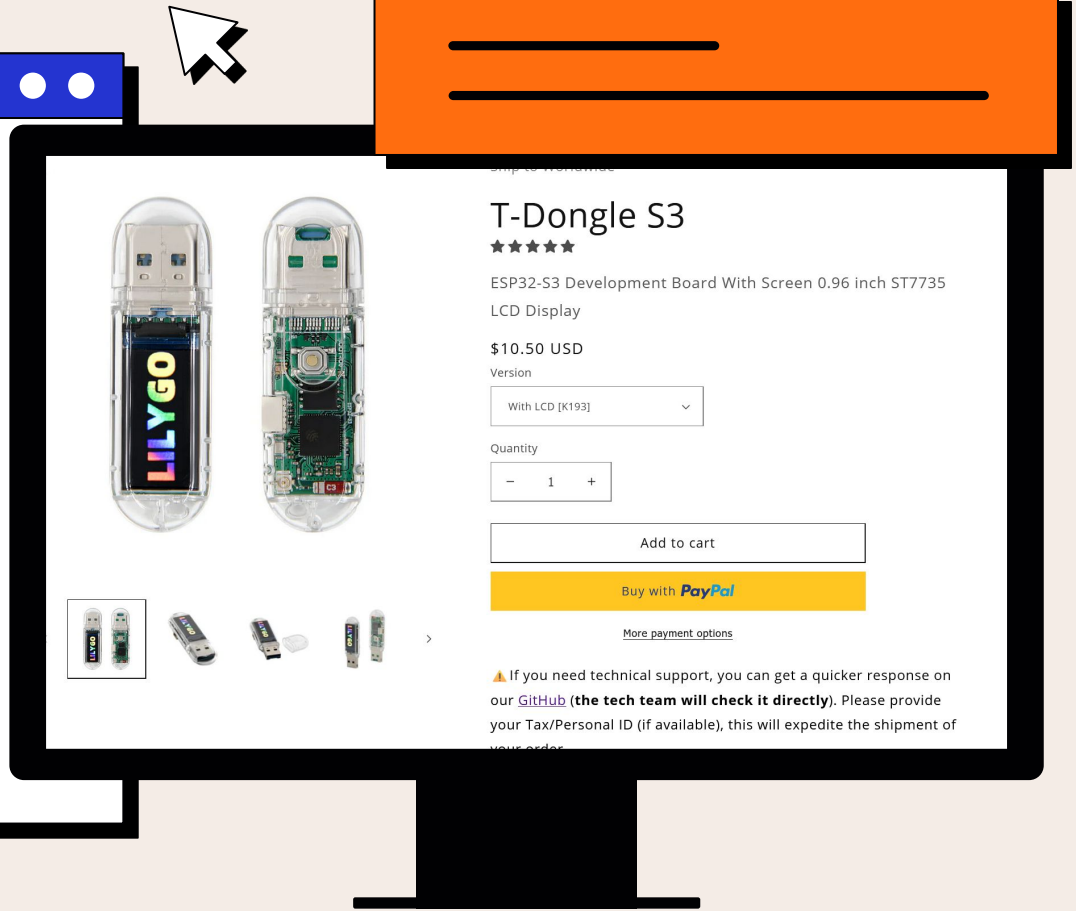
Tool Comparison

Requirement	Rubber Ducky	Flipper Zero	OMG Cable
USB			
Cheap			
Wireless Control			

* No control pre Oct 2023. Hold on we'll get there

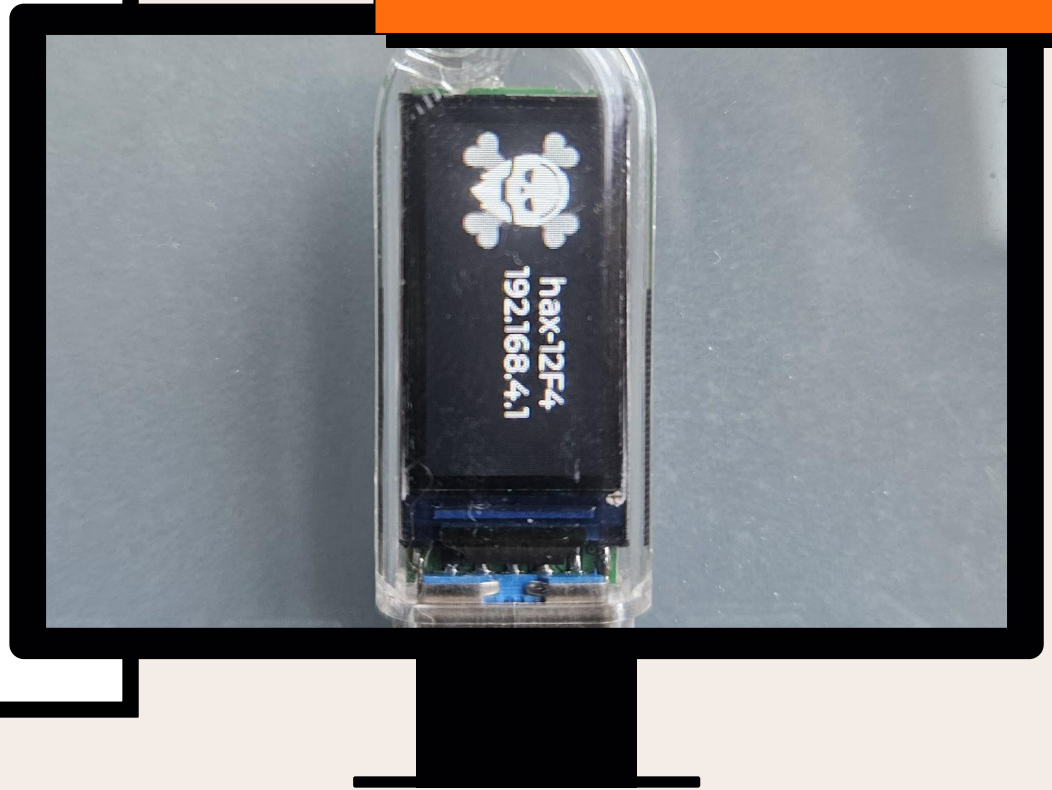
T-Dongle S3

- USB Formfactor
- Fancy color screen 12800 color pixels!
- WiFi and Bluetooth
- Program in C/C++, Micropython or Arduino



RadioJack

- Emulates Keyboard and Mouse
- Hosts its own Wifi server
- Telnet interface
- Allows random payloads or built in remote shell
- Re-flashable
- Laughing skull animation!
- Arduino code: radiojack.io



Why Arduino?

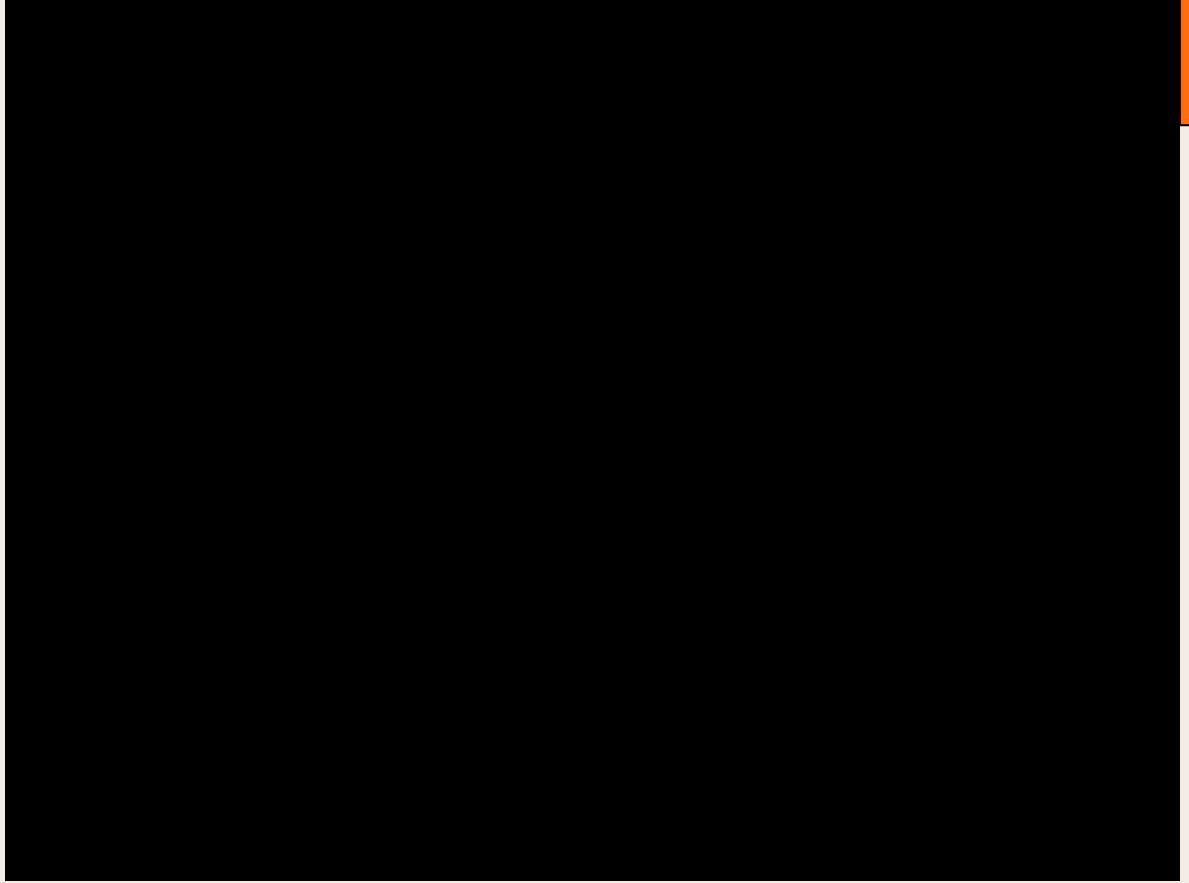


- The drivers just worked
- HID Libraries
- Wifi libraries

- Prove how easy it is
  - High Schoolers learn this

How to Use

- Plug USB in to target
- Connect to the SSID displayed on the screen
  - Enter “thepassword”
- Telnet to the IP shown on screen
- Follow command line interface prompts
- Features:
  - Drop payload that opens remote powershell prompt
  - Type as a keyboard
  - COM port Serial connection



Powershell PoC Video


WASTED
Target
Attacker

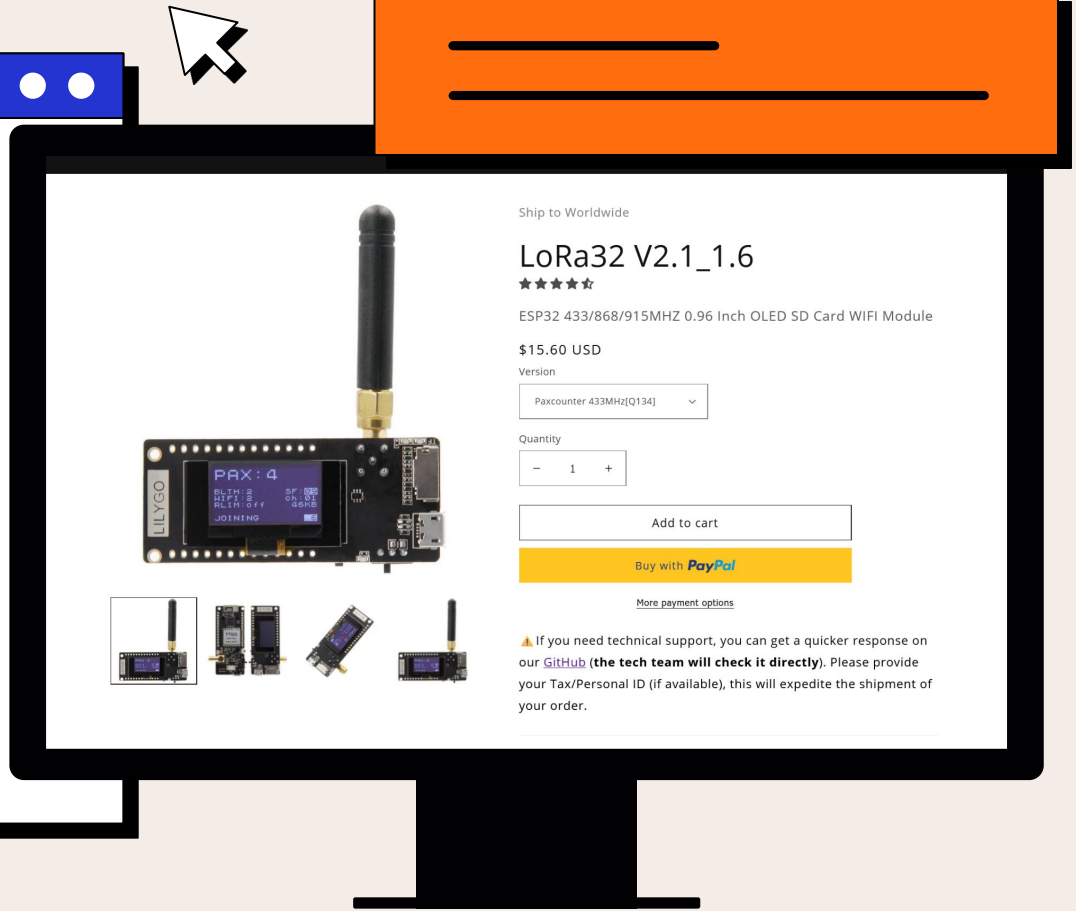
OMG Cable Stealthlink

- Looks like regular USB Cable
- Backdoor terminal using HIDX packets instead of COM port
- Sexy Marketing and ready to buy
- Way better than my hobby project



Lora S3

- Still Cheap
- Still Screen…ish
- Still WiFi and Bluetooth
- Still Program in C/C++, Micropython or Arduino
- LoRa!1!one!!



LoRa

- Low power long distance radio
- No license needed
- Theoretical Ranges of 3+ miles
- Requires Line of sight



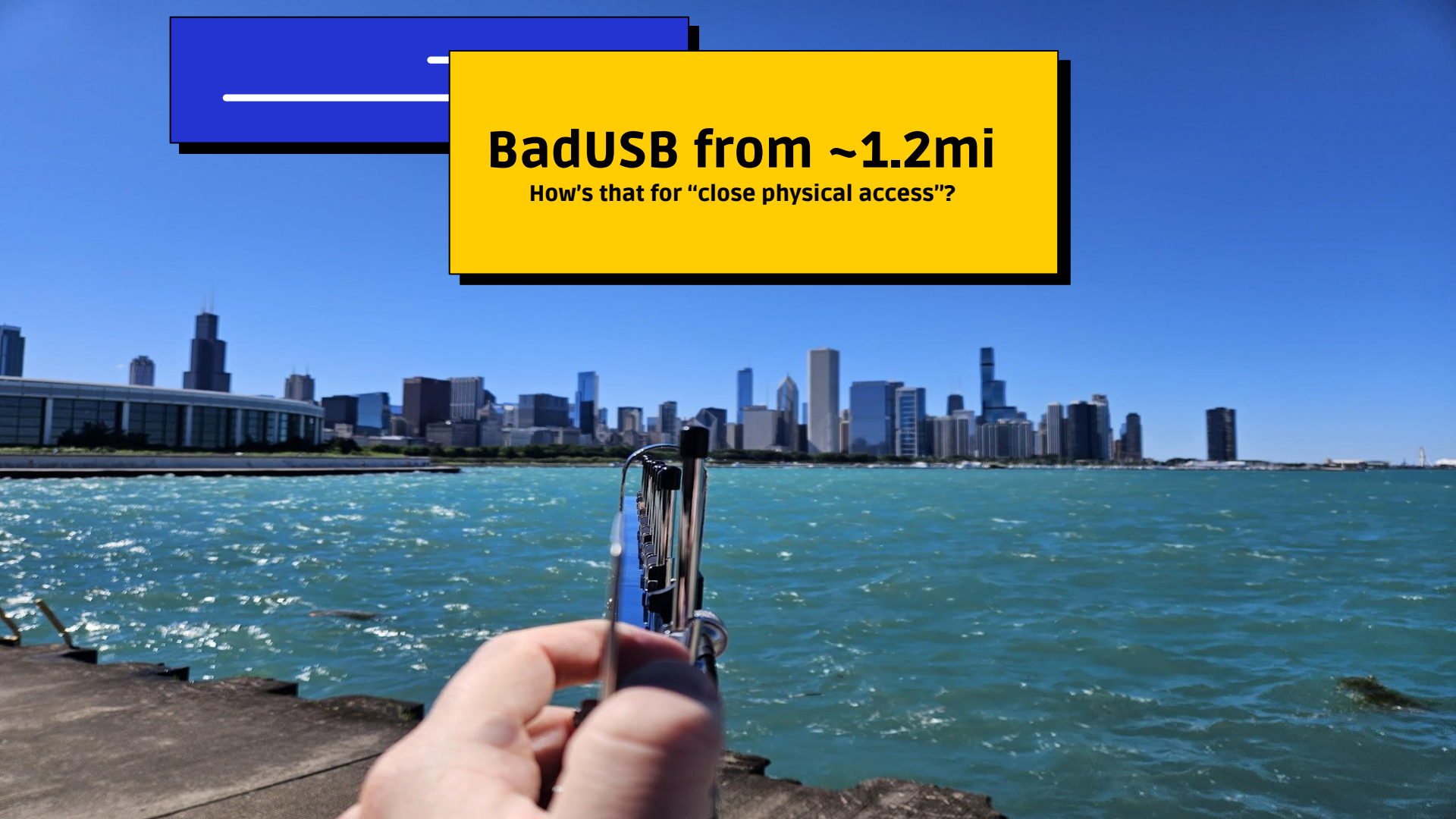
How to Use

(same as wifi)

- Connect to the SSID displayed on the screen
- Telnet to the IP shown on screen
- Follow command line interface prompts
- Features:
  - Drop payload that opens remote powershell prompt
  - Type as a keyboard
  - COM port Serial connection

BadUSB from ~1.2mi

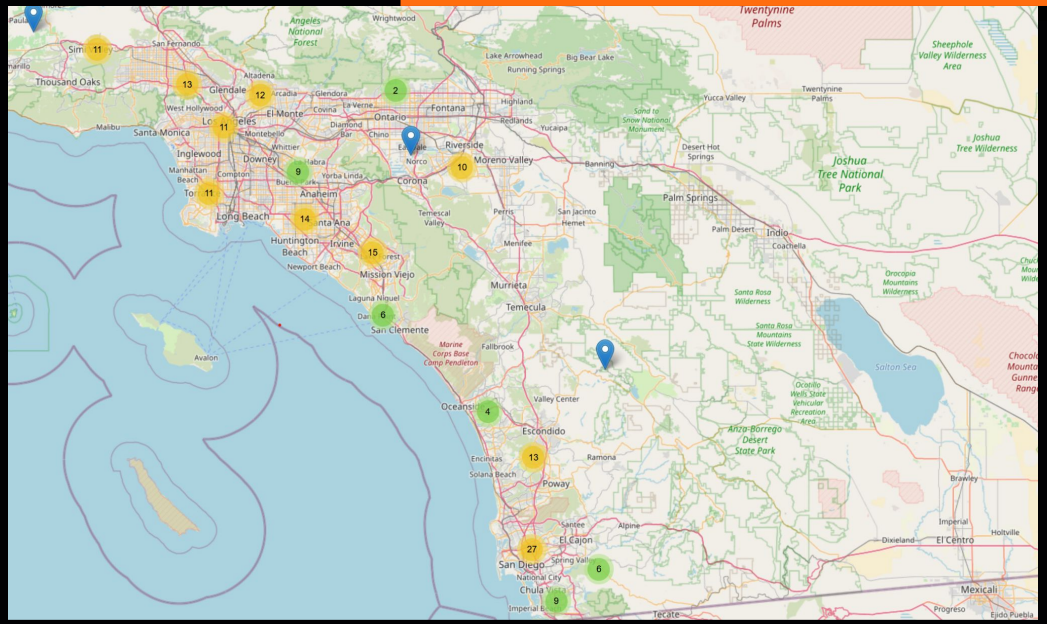
How's that for "close physical access"?



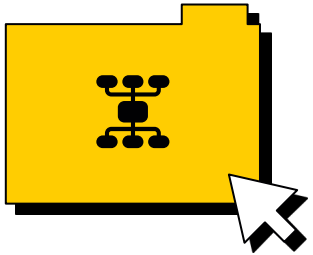
Can we take it further?

- Multi-hop Meshtastic network?
- Wifi bridge?
- What ideas do YOU have?

Takeaway is: You only need a few minutes and a few dollars to exploit exploit BadUSB.

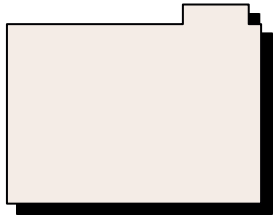


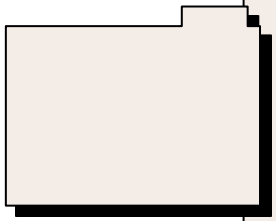
Mitigations

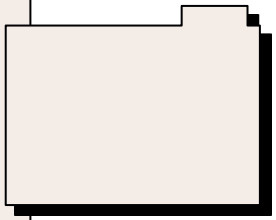


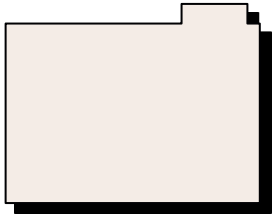
Hardware

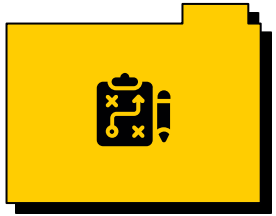
Cover your USB ports!
It’s that simple











Software

Disable USB stack. Require authentication to enable it.

Thank you!

Questions?

Code at: radiojack.io
Email: defcon@radiojack.io



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

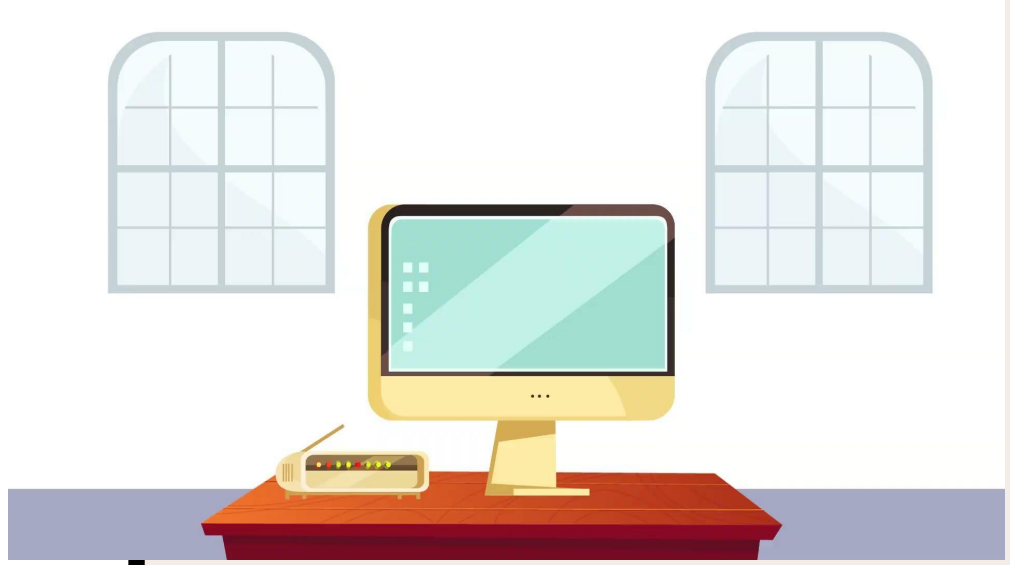
Additional artwork by Varx

More about the topic

Mercury is the closest planet to the Sun and the smallest one in the entire Solar System. This planet's name has nothing to do with the liquid metal, since Mercury was named after the Roman messenger god. Despite being closer to the Sun than Venus, its temperatures aren't as terribly hot as that planet's. Its surface is quite similar to that of Earth's Moon, which means there are a lot of craters and plains

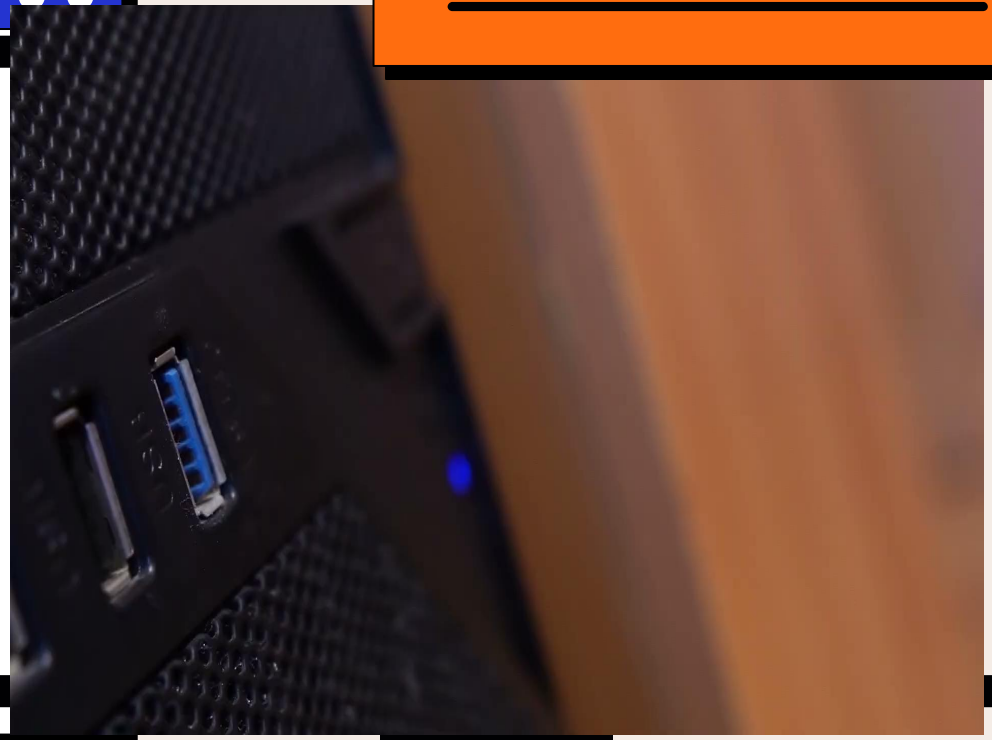
Speaking of craters, many of them were named after artists or authors who made significant contributions to their respective fields. Mercury takes a little more than 58 days to complete its rotation, so try to imagine how long days must be there! Since the temperatures are so extreme, albeit not as extreme as in Venus, and the solar radiation is so high, Mercury has been deemed to be non-habitable for humans

Long-Range Hacks: Risk for Under $20



USB Port Vulnerability

- Desolder or Cover your USB ports!



The slide title goes here!

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!

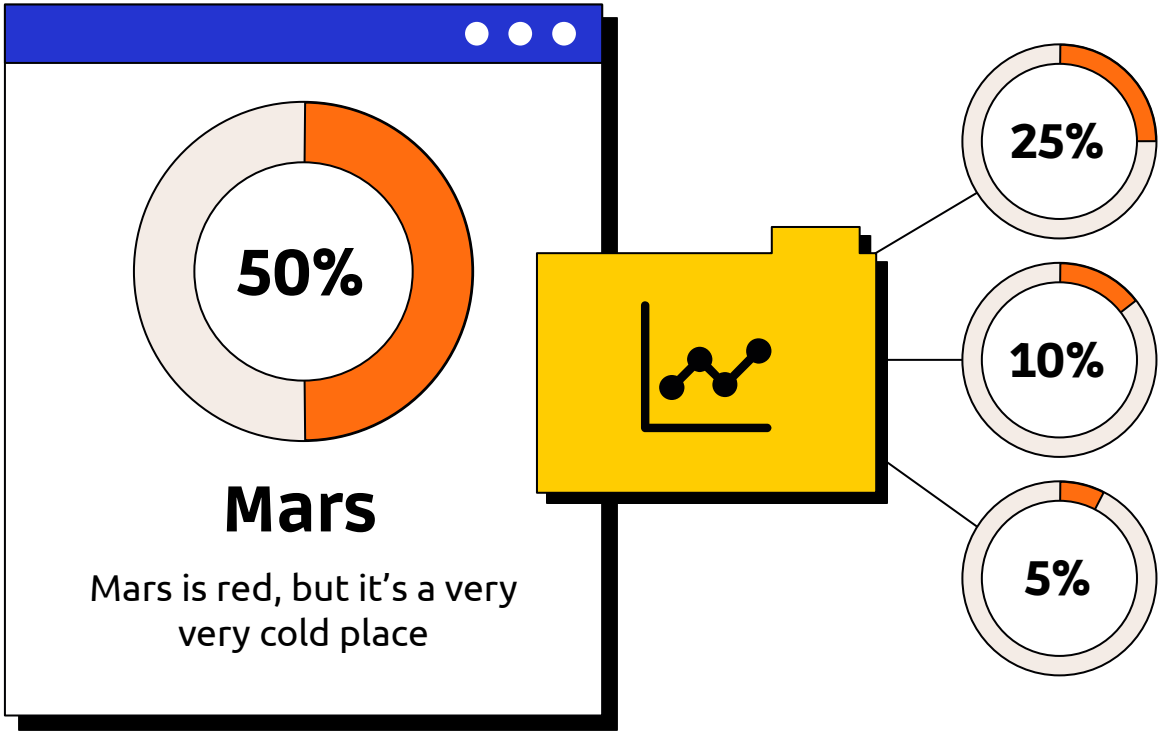
And the most important thing:
the audience won’t miss the point of your presentation

A picture always reinforces the concept

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



Core values



Mars

Mars is red, but it’s a very very cold place

Jupiter

Jupiter is the biggest planet of them all

Saturn

It’s composed of hydrogen and helium

Neptune

It’s the farthest planet from the Sun

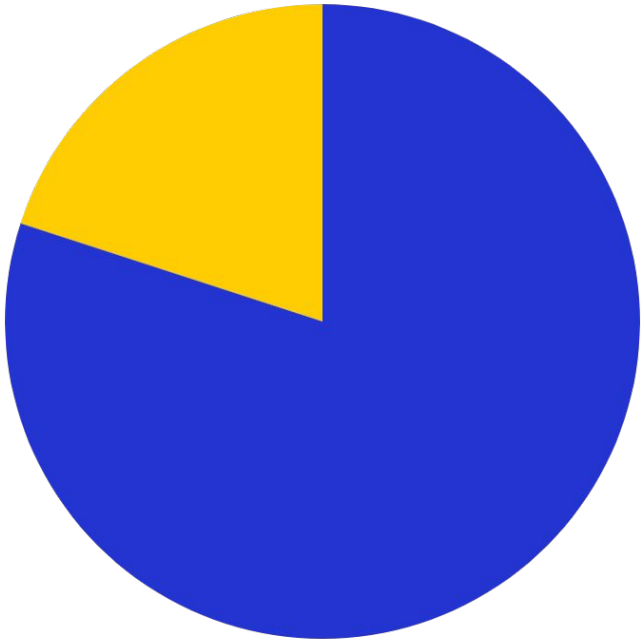
Segmentation

20%
Saturn

Saturn is the ringed one and a gas giant

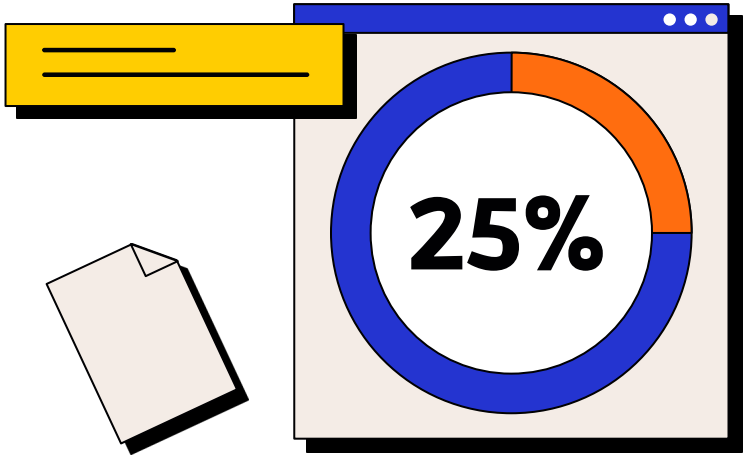
80%
Venus

Venus in fact has a very beautiful name



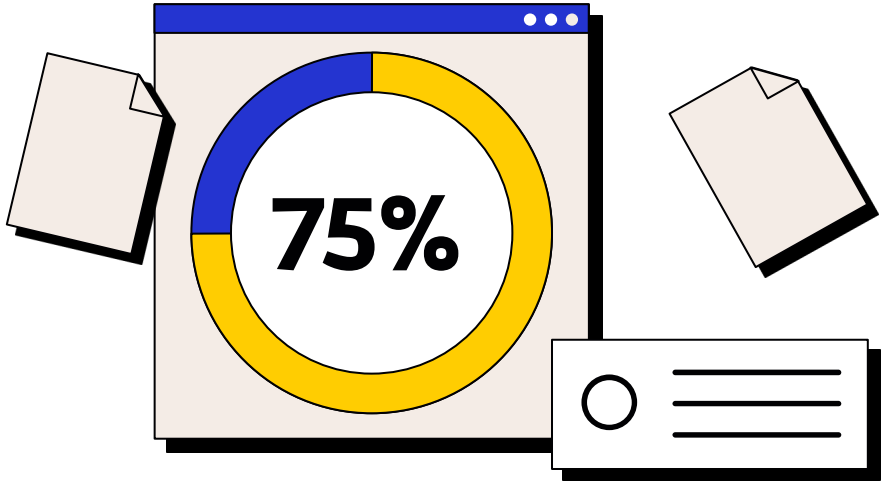
Follow the link in the graph to modify its data and then paste the new one here. For more info, **click here**

Comparisons



Mercury

Mercury is the smallest one in the Solar System but larger than Moon



Venus

It has a beautiful name and the second closest planet from the Sun

Fonts & colors used

This presentation has been made using the following fonts:

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

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



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



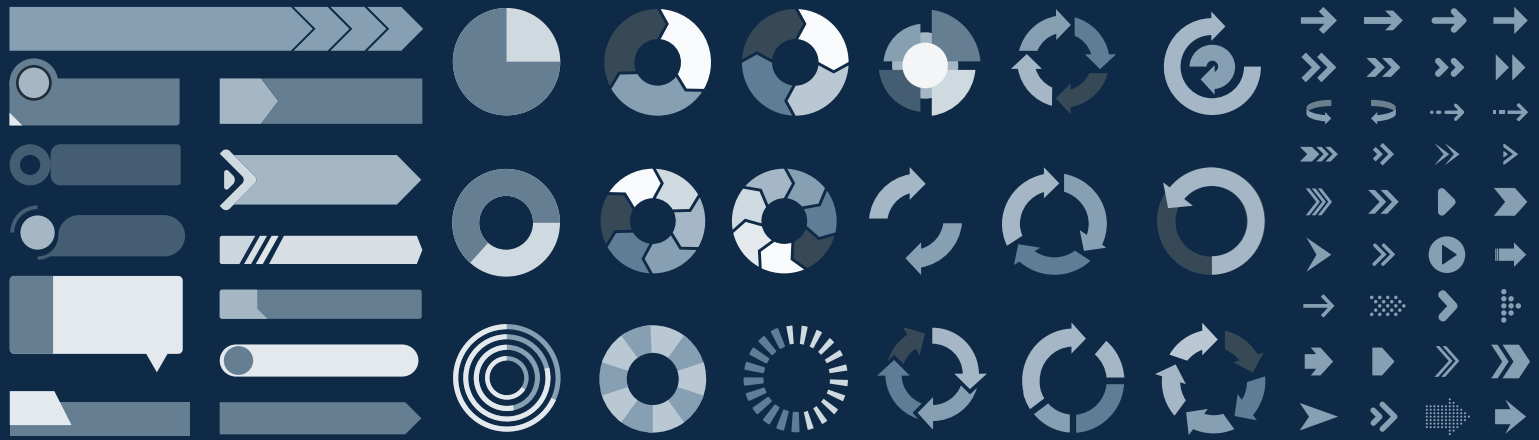
Rafiki

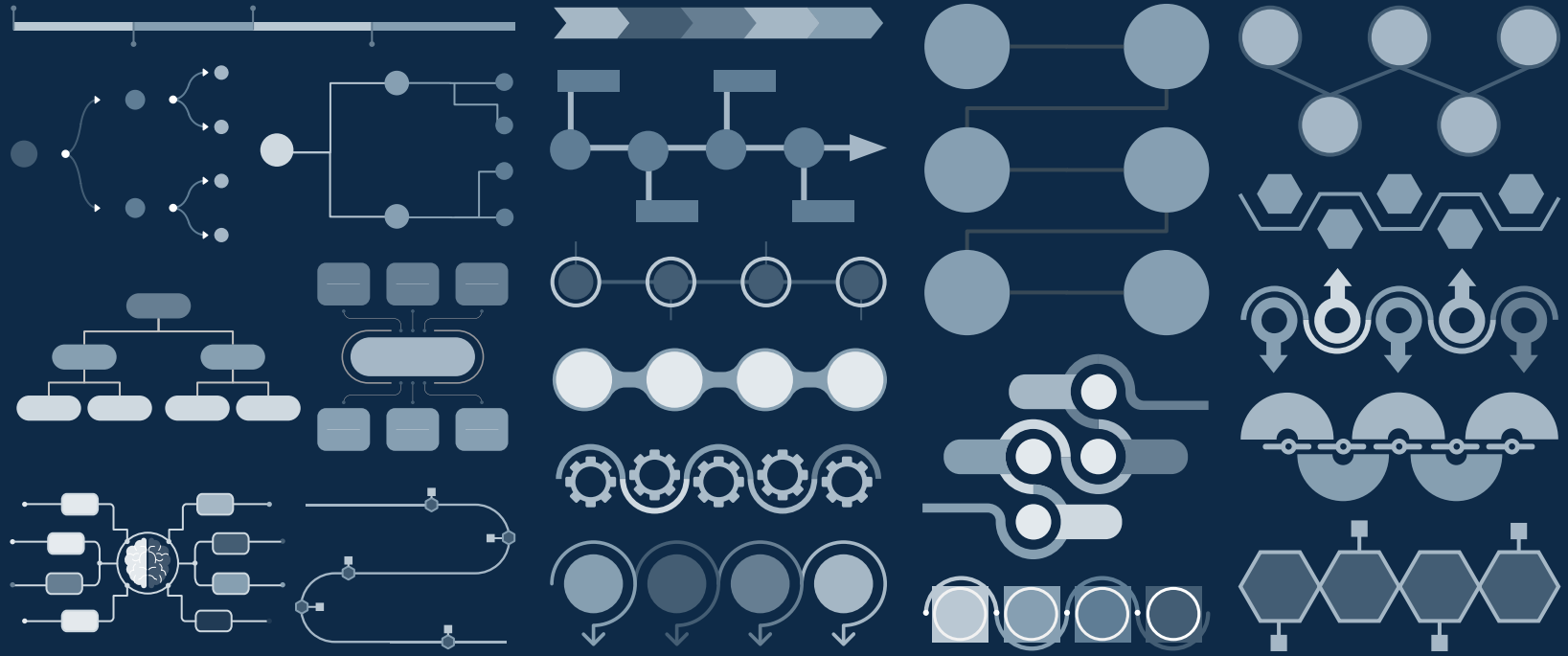


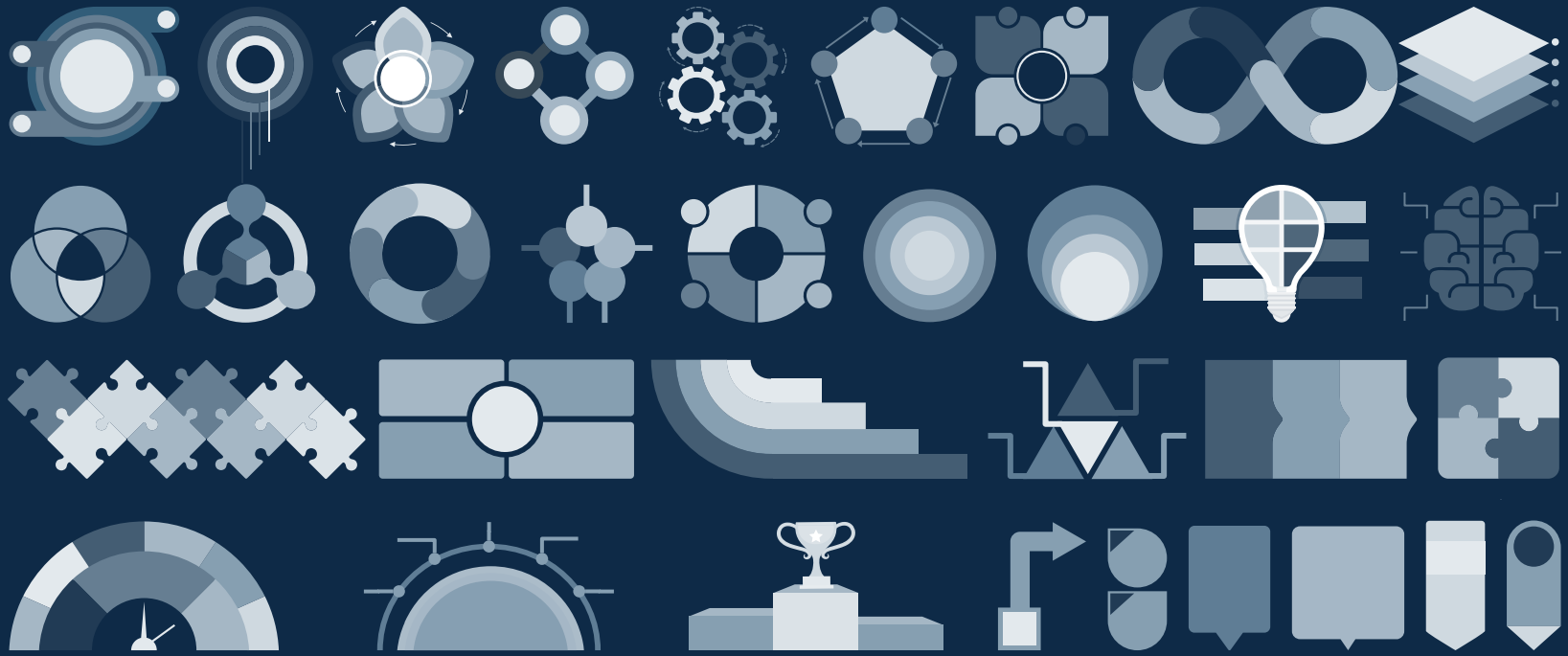
Cuate

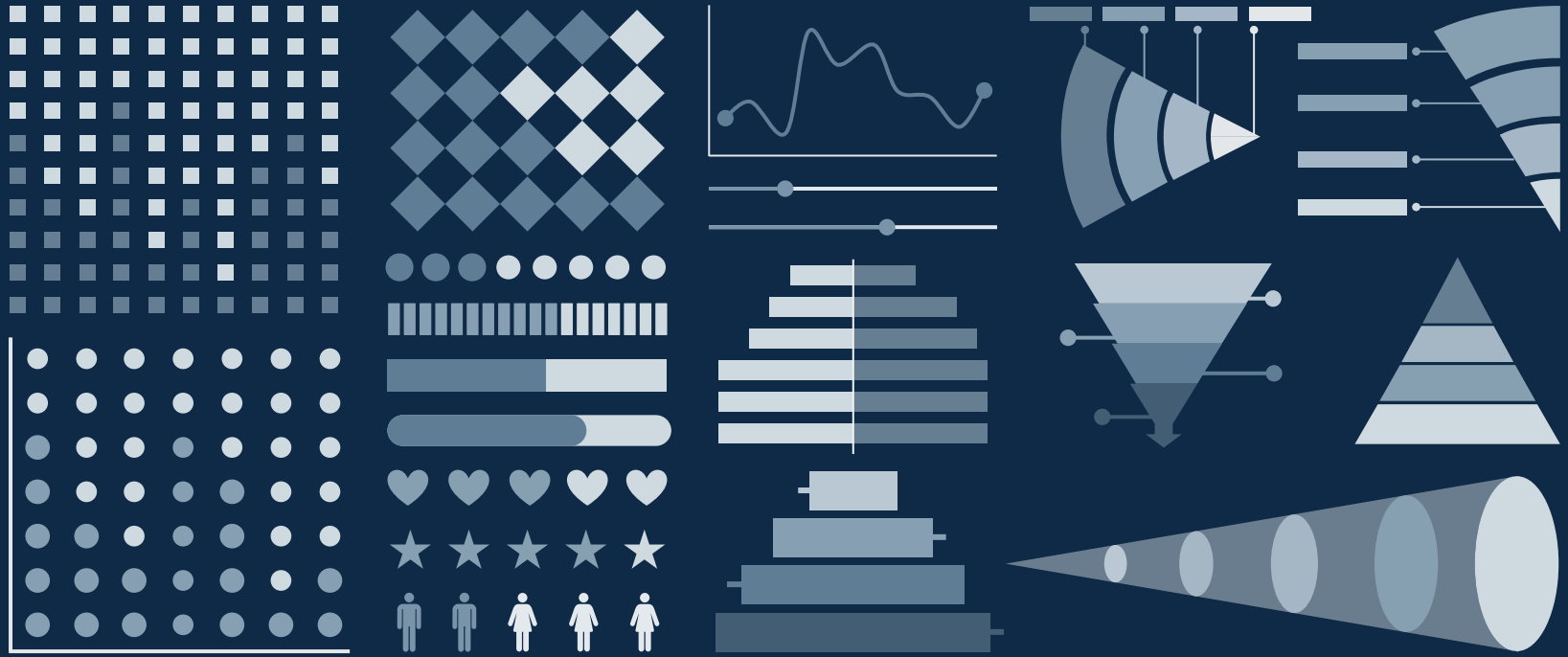
Use our editable graphic resources...

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.










slidesgo