

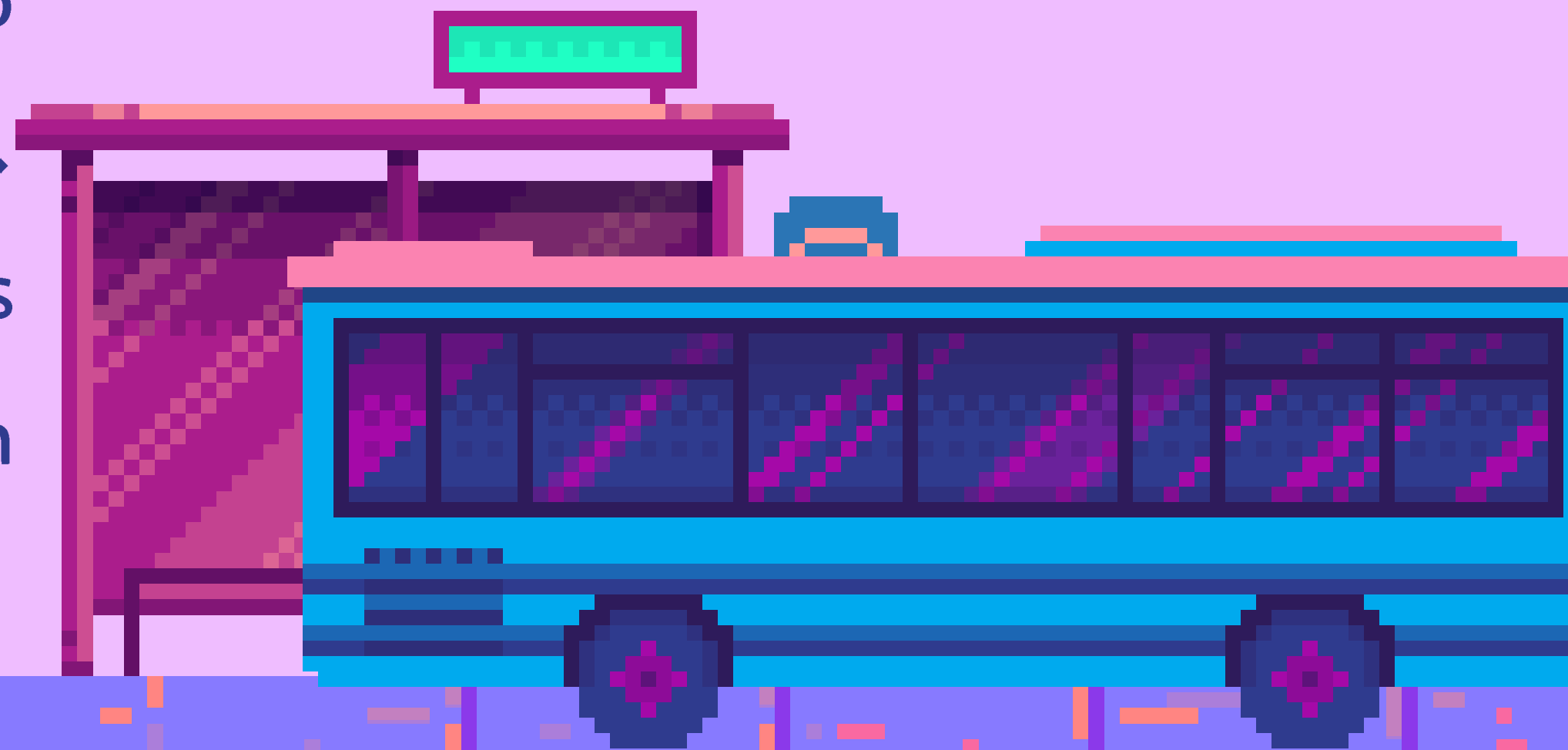
SEGURANÇA EM DISPOSITIVOS MÓVEIS

LET'S PLAY!



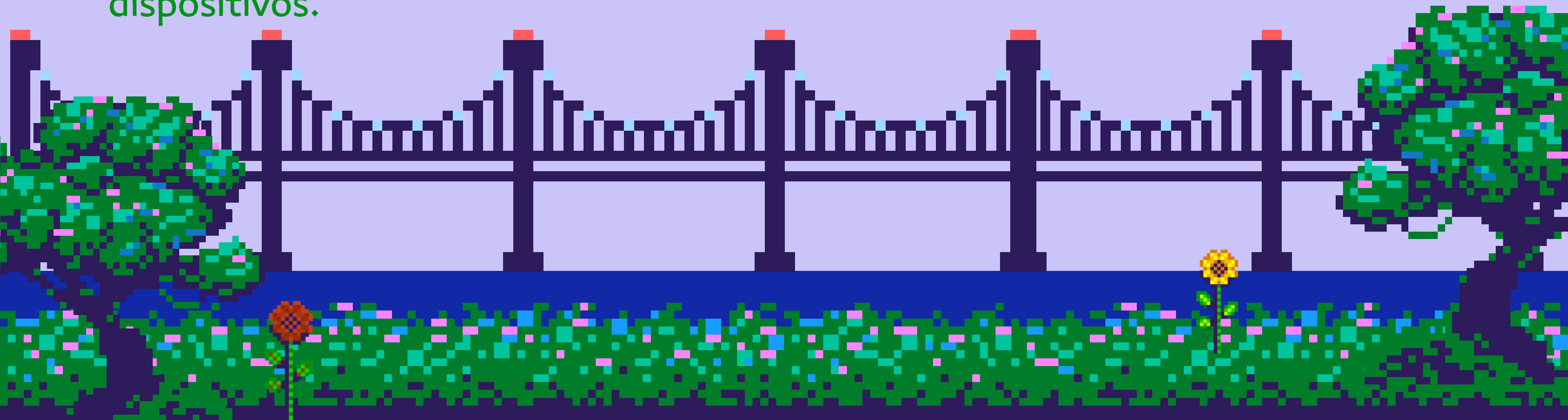
O QUE É?

A segurança em dispositivos moveis e a proteção dos dados e informações de dispositivos portáteis e das redes que estão conectada nesses dispositivos. Em sua maioria, os dispositivos moveis em uma rede incluem smartphones e tablets.



IMPORTÂNCIA

A importância se dá pelas medidas de segurança que são imprescindíveis para proteger os dados e as informações dos usuários, as mantendo sigilosas e não podendo ser acessados por hackers e pessoas mal-intencionadas, para evitar o vazamento e o roubo de dados e para que mantenha o desempenho dos dispositivos.





IOS E ANDROID

Android:

- Maior liberdade para controle e personalização.
- Maior variedade de fabricantes, modelos e preços à sua escolha.
- Inovação rápida devido à comunidade de desenvolvimento de código aberto.
- As atualizações automáticas são suaves e comunicadas de maneira clara.

Ios:

- É muito difícil adulterar seu software para fins maliciosos.
- A equipe dedicada, com foco em um único sistema para lançar atualizações.
- Padrões de segurança uniformes em uma gama limitada de dispositivos.
- Proteção de segurança FaceID disponível em todos os dispositivos mais recentes.





RISCOS ASSOCIADOS AO USO

As ameaças à segurança de dispositivos móveis aumentam todos os dias. Em 2014, a Kaspersky detectou mais de 3 milhões de malwares e segundo a IT Web, a quantidade de novos programas de malware detectados todos os dias ultrapassou 230.000, muitos sendo destinados a dispositivos portáteis. Algumas ameaças são:




RISCOS ASSOCIADOS AO USO

- Vazamento de dados: Aplicativos enviam dados pessoais para que sejam utilizados por anunciantes ou criminosos virtuais.
- Controle inadequado de sessão: Para facilitar as transações em dispositivos, muitos aplicativos utilizam-se de “tokens”, para que a identidade fique gravado a cada sessão, o controle inadequado da sessão acontece quando os aplicativos compartilham, acidentalmente, tokens de agentes mal-intencionados.



RISCOS ASSOCIADOS AO USO

- Wi-Fi sem proteção: Redes de Wi-Fi gratuitas costumam não ter proteção, podendo ter os dados invadidos pelos fornecedores.
- Falsificação de redes: Quando pessoas especialistas configuram falsos pontos de conexão, mas na verdade são armadilhas, para roubar as informações, muita das vezes pedindo para que faça login e as pessoas inserem as mesmas informações pessoais de outras contas.



MEDIDAS DE SEGURANÇA

Software antivírus: instale softwares antivírus em todos os dispositivos moveis, incluindo smartphones e tablets, para detectar e remover malwares do seu sistema.

Firewall: Instale um firewall em dispositivos moveis para bloquear o acesso não autorizado ao dispositivo e seus dados, assim dificultando o roubo de dados e atividades prejudiciais ao dispositivo.

Atualizações regulares: atualize regularmente o software antivírus e o sistema operacional do seu dispositivo para garantir proteção contra as ameaças mais recentes.

Criptografia: Use criptografia para proteger dados armazenados em dispositivos moveis, como e-mails, contatos e arquivos.





CÂMERAS DE SEGURANÇA

Os smartphones com câmera implementam várias medidas de segurança, como criptografia de ponta a ponta, autenticação, controle de acesso e armazenamento seguro de dados. Os aplicativos também possuem recursos de segurança próprios. Além disso, os sistemas operacionais recebem atualizações regulares para corrigir vulnerabilidades, garantindo a segurança contínua do dispositivo e dos seus dados.

MUITO OBRIGADO
PELA ATENÇÃO

PLAY AGAIN?

