

PROTEÇÃO DE DADOS NO CARNAVAL: COMO NOS RESGUARDAR



As celebrações carnavalescas são motivo de muita folia para a população brasileira. Contudo, é importante ter em mente que tais festividades também aumentam a ocorrência de crimes.

Portanto, com o aumento do uso de aplicativos, pagamentos digitais e redes sociais, a proteção de nossos dados pessoais e o cuidado com nossa privacidade devem ser redobrados.

Ao acessar locais públicos, é importante ter cuidado ao escanear "QR Codes", pois eles podem direcionar para sites maliciosos e acarretar em práticas danosas. Devemos evitar o preenchimento formulários suspeitos e o fornecimento de dados pessoais para desconhecidos. Evite postar imagens de ingressos que contenham informações sobre a reserva, para evitar fraudes.

Em seus aplicativos bancários e de redes sociais, utilize senhas fortes e, se possível ative a autenticação em dois fatores. Também é recomendado que você monitore suas transações e ative notificações para movimentações suspeitas.

Ao comprar produtos durante as celebrações, sempre confirme o valor da mercadoria e a identidade do vendedor ou estabelecimento. Em caso de pagamentos via Pix, cuidado com o uso de seu celular em ambientes muito expostos. Se perder seu celular, utilize ferramentas como "Encontre Meu Dispositivo" para bloquear o aparelho, evitando o uso por terceiros.

Mas acima de tudo, se beber, não dirija!

DADOS DE 39 MILHÕES DE PESSOAS PODEM SER SIDO VAZADOS APÓS ATAQUE AO SISTEMA CAT

Em 04.02.2025, o sistema de cadastro de Comunicação de Acidente de Trabalho (CAT) sofreu um ataque cibernético que possibilitou o vazamento de dados pessoais de 39 milhões de brasileiros.

O CAT tem por objetivo possibilitar a comunicação, pelos empregadores, de acidentes de trabalho, doenças ocupacionais ou casos de morte de seus colaboradores. Por sua natureza, diversos dados pessoais nesta base são informações de saúde, ou seja, dados sensíveis perante à LGPD.

Ainda, o agente responsável pelo incidente alegou que entrou em contato com representantes do "Dataprev", empresa pública responsável por gerir bases de dados do governo, para informar sobre o ataque previamente, e que não houve tentativa de solução.

No entanto, segundo o Dataprev, não foi identificado qualquer comprometimento na plataforma vinculada ao INSS, e que "trabalha com protocolos rigorosos e em conjunto com seus clientes para assegurar a segurança de seus sistemas".

MALWARE ENCONTRADO EM IPHONES PODE ROUBAR CRIPTOMOEDAS

Pesquisadores da *Kaspersky Lab*, uma empresa de segurança na internet, identificaram que alguns aplicativos exclusivos do iPhone estariam infectados com um malware capaz de identificar palavras-chave relacionadas ao uso criptomoedas, facilitando o roubo destes ativos através do envio destas informações aos invasores.

Chamado de "*SparkCat*" pelos pesquisadores, o malware está ativo desde março de 2024, no entanto, não se sabe se a infecção é resultado de um ataque por terceiros, ou uma iniciativa premeditada pelos desenvolvedores dos aplicativos infectados.



Segundo a *Kaspersky Lab*, a melhor forma de se proteger contra este tipo de malware é instalar apenas aplicativos que estejam disponíveis em lojas oficiais dos dispositivos, que contenham muitas avaliações positivas, milhões de número de downloads, e que tenham sido disponibilizados há pelo menos vários meses.

GOVERNOS PROÍBEM O USO DO DEEPSEEK. INVESTIDORES, ABRAÇAM.

O "*DeepSeek*", uma inteligência artificial em chatbot de origem chinesa, teve seu uso proibido por entidades governamentais de alguns países mundo afora.

A Austrália proibiu a utilização da IA em dispositivos governamentais, sob a alegação de que a ferramenta apresenta "um risco inaceitável à segurança nacional". O Canadá também proibiu o uso da IA em dispositivos do governo federal, e orientou que departamentos governamentais adotem a mesma medida.

Outras instituições governamentais de diferentes países também restringiram a instalação e uso da tecnologia, como em Taiwan, na Itália, nos Países Baixos e nos Estados Unidos.

Contudo, estrategistas do *Morgan Stanley*, do *JPMorgan* e do *UBS Group*, grandes players de *Wall Street*, estão demonstrando apoio à IA chinesa, e esperam que os ganhos de ações estimulados por este modelo de inteligência artificial continuem.

"Os investidores globais estão começando a reavaliar a viabilidade de investir da China no campo de tecnologia e IA, após um longo período de atenção limitada", escreveram estrategistas do *Morgan Stanley*.

A fabricante de carros *BYD* anunciou que o sistema de direção autônoma de seus carros será alimentado pelo *DeepSeek*, alegando que a presença da IA trará aprimoramentos à condução autônoma, fazendo com que esse tipo de tecnologia se torne uma ferramenta indispensável no futuro.