



OPINIÃO

Trocar de celular todo ano ainda vale a pena? Ciclo de uso se aproxima de quatro anos

Stephanie Peart (*)

Durante anos, o mercado de smartphones funcionou em torno de uma lógica simples: a cada nova geração, surgia um motivo para trocar de aparelho. Uma câmera melhor, um processador mais rápido, uma tela mais avançada ou algum novo recurso ajudavam a sustentar o ciclo de renovação.

Mas esses argumentos começam a perder força. Os smartphones chegaram a um nível de maturidade tecnológica em que, para muitos consumidores, um aparelho de dois ou três anos ainda atende bem às tarefas cotidianas. Redes sociais, aplicativos bancários, streaming, mensagens, fotografia e ferramentas de trabalho continuam funcionando em dispositivos que já não são os mais recentes do mercado.

Segundo a Counterpoint Research, o ciclo global de substituição dos smartphones está se aproximando de quatro anos, tendência que deve continuar em 2026 e 2027. A consultoria relaciona esse movimento ao aumento dos preços provocado pelos custos de memória e outros componentes. A maturidade dos aparelhos e as diferenças cada vez mais incrementais entre algumas gerações também ajudam a reduzir a urgência da troca.

Ao mesmo tempo, os smartphones ficaram mais caros. Quando o custo de uma troca aumenta e a diferença de experiência entre duas gerações diminui, a decisão de substituir o celular deixa de ser automática. O consumidor passa a perguntar o que realmente ganharia trocando o aparelho naquele momento.

Para a indústria, isso representa uma mudança importante. Se antes era suficiente convencer o consumidor de que o próximo aparelho era melhor, agora será necessário mostrar em quais características ele é significativamente superior.

A inteligência artificial pode ser parte dessa resposta, mas

um novo recurso só estimula a troca quando oferece uma diferença perceptível na rotina. A presença da tecnologia no aparelho, por si só, não garante que o consumidor reconheça valor suficiente para pagar por uma nova geração.

Por isso, talvez estejamos entrando em uma fase de menos trocas automáticas e mais tempo de uso. Isso não significa necessariamente menos oportunidades para o mercado. Um consumidor que permanece mais tempo com o mesmo smartphone tende a dar mais importância a seguro, assistência técnica, reparo, substituição da bateria e serviços que preservem o funcionamento e o valor do aparelho.

Modelos de assinatura também precisam acompanhar essa transformação. A possibilidade de trocar o aparelho pode continuar existindo, mas não precisa ser tratada como uma obrigação anual. O valor do serviço passa a estar também na proteção, na assistência e na liberdade de escolher entre continuar com o dispositivo ou fazer a substituição quando houver uma necessidade real.

É uma mudança de perspectiva. O sucesso de um smartphone pode deixar de ser medido apenas pelo número de unidades vendidas em cada lançamento e passar a considerar quanto tempo o dispositivo permanece relevante, reparável e útil — inclusive quando passa de um usuário para outro.

A indústria terá de se adaptar a um consumidor menos impulsivo e mais racional. Em vez de criar uma necessidade de troca a cada ano, terá de construir valor suficiente para que uma nova geração represente, de fato, um salto.

O smartphone pode estar ficando bom demais para ser trocado todo ano. E talvez essa seja uma boa notícia. O desafio daqui para frente será fazer cada aparelho durar mais e valer mais a pena enquanto estiver em suas mãos.

(*) CEO da Leapfone, startup pioneira no conceito de Phone as a Service e na oferta de smartphones como novos por assinatura. - E-mail: leapfone@nbpress.com.br.



News@TI

Teletex firma parceria com Vectra AI

@A Teletex, integradora brasileira de tecnologia com 40 anos de mercado, anuncia uma parceria com a Vectra AI, empresa especializada em segurança e observabilidade baseadas em inteligência artificial. O acordo incorpora ao portfólio da Cybercare, unidade de cibersegurança da Teletex, recursos avançados de Network Detection and Response (NDR) voltados à identificação e interrupção de ataques em ambientes híbridos e multicloud. A parceria combina a tecnologia e a expertise da Vectra AI em detecção e resposta a ameaças com a presença nacional, a capacidade de integração e os serviços da Teletex. As empresas atuarão de forma complementar ao longo da jornada dos clientes, desde a adoção e implementação das soluções até o uso da plataforma e a evolução das estratégias de detecção e resposta a ameaças.

SuperApp russo torna-se elemento de controle da sociedade

SuperApps, ou superaplicativos, são plataformas que reúnem múltiplas funcionalidades em um único software, dispensando a necessidade de baixar diversos aplicativos diferentes.

Vivaldo José Breternitz (*)

Nos últimos meses, usar a internet na Rússia tornou-se algo cada vez mais controlado pelo governo: WhatsApp e Telegram enfrentam novas restrições, VPNs tem sido bloqueadas e, desde setembro de 2025, os novos smartphones e tablets vendidos no país trazem um SuperApp pré-instalado destinado a concentrar grande parte das comunicações e dos serviços cotidianos como operações bancárias e acesso a serviços públicos.

Esse SuperApp, chamado Max, nasceu com a promessa de simplificar a burocracia, mas segundo o jornal britânico *The Guardian*, vai muito além: consegue capturar telas e acessar informações sobre as transações efetuadas por seus usuários; foi desenvolvido pela VK, grupo russo proprietário da rede VKontakte e estreitamente ligado ao governo.

Nos últimos 18 meses, as autoridades aceleraram sua difusão, apresentando-o como alternativa nacional ao Telegram e ao WhatsApp. Funcionários públicos, professores, estudantes e escolas são pressionados a utilizar a plataforma, o que fez, a partir de meados desse ano, o Max tornar-se o aplicativo mais usado no país.



mediaphotos_CANVA

O crescimento do Max coincide com o fechamento progressivo do espaço digital russo, fazendo com que uma fatia crescente das comunicações e dos serviços cotidianos passe por infraestruturas controladas pelo governo, evidenciando um ataque à democracia, como denuncia a Human Rights Watch, ONG internacional focada na investigação, defesa e promoção

dos direitos humanos em todo o mundo.

Final, regular e controlar as redes sociais e as plataformas digitais é o sonho de todo governo com vocação totalitária.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitzz@gmail.com.

Password spraying transforma senhas comuns em porta de entrada para ataques

Nem todo ataque cibernético precisa testar milhares de combinações até descobrir uma senha. Em alguns casos, os criminosos fazem justamente o contrário: escolhem poucas senhas, normalmente entre as mais comuns e previsíveis, e tentam utilizá-las em uma grande quantidade de contas. É assim que funciona o chamado *password spraying*.

A estratégia explora um problema antigo da segurança digital que continua atual: o uso de credenciais fracas ou repetidas. Combinações como “123456”, “admin” e outras senhas previsíveis podem parecer erros básicos, mas continuam representando uma oportunidade para invasores.

A diferença em relação a um ataque tradicional de força bruta está justamente na forma de atuação. Em vez de realizar inúmeras tentativas contra uma única conta, comportamento que tende a acionar mecanismos de bloqueio, o *password spraying* distribui as tentativas entre diferentes usuários. Isso pode dificultar a identificação da atividade maliciosa e permitir que o ataque permaneça mais tempo sem ser percebido.

O problema não se restringe às senhas escolhidas pelos funcionários. Credenciais padrão mantidas em equipamentos, aplicações, firewalls, pontos de acesso e outros componentes da infraestrutura também podem ampliar a superfície de ataque de uma organização. Por isso, tratar segurança de credenciais apenas como uma responsabilidade individual do usuário é insuficiente. A medida que uma empresa acumula sistemas, aplicações e diferentes níveis de acesso, a gestão dessas identidades passa a ser uma questão de segurança corporativa.

Um dos principais mecanismos de proteção é a adoção de senhas longas, únicas e difíceis de adivinhar. A reutilização da mesma credencial em diferentes serviços merece atenção especial: quando uma senha é comprometida, o risco pode se espalhar para outras contas nas quais a mesma combinação tenha sido utilizada.



Divulgação ADDEE

Rodrigo Gazola, CEO da ADDEE.

A autenticação multifator acrescenta outra barreira importante. Mesmo que um criminoso consiga descobrir uma senha válida, ainda precisará superar uma segunda etapa de autenticação. Para contas com acesso a informações sensíveis ou privilégios administrativos, essa camada se torna ainda mais relevante.

Também é necessário olhar para o comportamento da rede. Uma tentativa isolada de autenticação pode não despertar atenção. Diversas tentativas semelhantes distribuídas entre diferentes contas, entretanto, podem revelar um padrão. Monitoramento de logs, políticas de acesso e mecanismos capazes de identificar comportamentos anormais são fundamentais para perceber esse tipo de movimentação.

Há ainda um componente humano que nenhuma tecnologia resolve sozinha. Funcionários precisam entender por que não devem reutilizar credenciais, como reconhecer tentativas de obtenção de senhas e qual procedimento seguir quando suspeitam que uma conta tenha sido comprometida.

O tamanho desse risco pode ser percebido nos bancos de dados que reúnem informações sobre vazamentos já conhecidos. O *Have I Been Pwned*, por exemplo, permite

consultar se determinado endereço de e-mail apareceu em incidentes públicos e também verificar se uma senha já foi encontrada em bases de credenciais expostas.

O histórico mostra por que esse cuidado importa. Em 2013, um ataque contra a Adobe comprometeu dados de milhões de contas, incluindo informações relacionadas a usuários e senhas. Casos dessa dimensão ajudaram a formar enormes bases de credenciais que podem posteriormente ser utilizadas por criminosos em novas tentativas de invasão.

Isso cria um efeito em cadeia. Uma senha exposta anos atrás pode continuar representando risco hoje caso ainda seja utilizada pelo mesmo usuário em algum serviço. O problema deixa de estar restrito à empresa originalmente atacada e acompanha a credencial enquanto ela continuar ativa.

O *password spraying* mostra que cibersegurança nem sempre é uma disputa envolvendo técnicas extremamente sofisticadas. Muitas vezes, o invasor procura justamente o caminho mais simples: uma senha previsível, uma credencial esquecida ou uma conta sem proteção adicional.

A resposta, portanto, também precisa começar pelo básico bem executado. Senhas únicas e robustas, autenticação multifator, gestão adequada de credenciais, monitoramento de acessos, treinamento das equipes e políticas claras de segurança precisam funcionar em conjunto.

Nenhuma dessas medidas, isoladamente, elimina o risco. Segurança cibernética depende de camadas. E quanto mais difícil for para um invasor transformar uma única credencial comprometida em acesso à infraestrutura da empresa, menor será a chance de uma senha aparentemente banal se tornar o início de um incidente muito maior.

(Fonte: Rodrigo Gazola é CEO da Addee, empresa especializada em soluções de tecnologia e cibersegurança).

Editoriais

Economia: Nelson Tucci (nelson.tucci@netjen.com.br)
Mercado/Negócios/Tecnologia/Agronegócios/ Espaço empresarial: Ricardo Souza (ricardosouza@netjen.com.br);
Livros: Ralph Peter (ralphpeter@agenteliterarioralph.com.br)
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.