

WhatsApp é plataforma mais citada em boletins de ocorrência no Estado de SP

Até menos 9.645 pessoas sofreram golpes, entre os mais de 75 mil casos de estelionato digital e invasão de celular registrados no Estado

O paulistano Kenzo Yama recebeu em uma manhã de maio um gif com mensagem de "te amo" de alguém que declarava ser sua mãe. O número diferente logo chamou a sua atenção e o fez questionar o interlocutor.

A réplica com uma sequência de erros ortográficos aumentou a suspeita. Yama se antecipou ao golpista e pediu dinheiro, o que fez o estelionatário desistir da conversa. O relato, com prints da conversa, foi divulgado na rede social Reddit.

Diferentemente de Yama, ao menos outras 9.645 pessoas sofreram golpes no WhatsApp, entre os mais de 75 mil casos de estelionato digital e invasão de celular registrados no estado de São Paulo. A plataforma é a mais citada, à frente de Instagram (8.061), Facebook (1.229), "aplicativos de mensagem" (1.083) e aplicativos de relacionamento (75).

Os dados sobre os 75.102 casos de invasão de celular e outros delitos digitais no Estado de São Paulo entre janeiro de 2019 e abril deste ano são publicados pela primeira vez pela reportagem, que os obteve via Lei de Acesso à Informação.

São estatísticas ausentes, por exemplo, do Anuário Brasileiro de Segurança Pública, o principal compêndio nacional de dados públicos sobre crimes, uma vez que o estado de São Paulo não os divulga. Isso porque a Secretaria de Segurança Pública (SSP) não produz informação oficial sobre esses crimes, segundo nota da pasta enviada à reportagem.

Não há uma metodologia para registro de local nesses crimes que discrimine se o termo se refere ao espaço físico ou digital. Os locais mais citados são "outros" (31.427) e "via pública" (13.429).

No caso do roubo de identidade, criminosos baixam imagens e consultam informações sobre os contatos da vítima no Facebook e em outras redes sociais para se passar por um parente ou amigo.

Outros golpes circulam no WhatsApp, como a divulgação de links maliciosos (criados apenas para permitir golpes) e propostas de empregos falsas.

Na capital paulista, à qual se referem 31% dos boletins de ocorrência, a plataforma mais citada é o Instagram, em 2.562 vezes. O WhatsApp fica em segundo, com 2.047. A capital paulista tem 25,78% da população do estado, mostra o censo de 2022.

No Instagram, criminosos também roubam identidades, usam deep fakes (vídeos falsos que parecem verídicos) para divulgar ofertas de falsos investimentos e se passam por sugar daddys (homens em geral maduros que se oferecem para sustentar moças mais jovens). Eles também usam a rede para levar vítimas a links maliciosos ou para coletar transferências sob pretexto de bons negócios.

O número de crimes digitais explodiu em abril de 2020, quando quase triplicou em relação ao registrado a março na capital e no estado de São Paulo, no início do isolamento social em decorrência da pandemia de Covid.

Foi apenas em dezembro de 2020 que o então governador João Dória inaugurou a Divisão de Crimes Cibernéticos da Polícia Civil. Nesse ponto, a série histórica dos delitos digitais subiu mais uma vez, o que indica uma subnotificação anterior.

Nos casos de golpe nas redes sociais, a vítima precisa tirar prints, fazer vídeos e guardar imagens que podem servir como pistas na investigação ou até configurar flagrante.

Entre janeiro de 2019 e abril deste ano, apenas oito a cada



No caso do roubo de identidade, criminosos baixam imagens e consultam informações sobre os contatos da vítima no Facebook e em outras redes sociais

Opções de segurança

Os usuários têm opções para se proteger no próprio app de mensagens, como autenticação em duas etapas, recursos de privacidade e de recuperação de conta. Veja como ativá-las abaixo. Com a autenticação de dois fatores, o usuário cria uma senha numérica adicional, pedida pelo WhatsApp, que será pedida após a confirmação do número de telefone. Também é possível ativar a opção de

bloqueio no WhatsApp. Esse recurso libera acesso ao aplicativo mediante reconhecimento biométrico do próprio smartphone, via reconhecimento de digital ou da face. Outra opção de privacidade do WhatsApp é a escolha de quem pode ver a foto de perfil. Essa imagem de identificação pode ser roubada por criminosos, que tentam se passar pela pessoa para pedir dinheiro a familiares e amigos.

Em qualquer caso de golpe, as autoridades recomendam o registro de boletim de ocorrência

dez mil casos de crimes digitais eram flagrante, o que diminui a chance de investigação prosseguir. A subnotificação, além disso, é um desafio no combate ao crime digital.

A polícia não precisa estar ao lado da vítima do lado do golpe. As pessoas podem apitar o trabalho da polícia quando percebe a fraude, se tirar um print ou gravar o episódio, para configurar o flagrante.

É possível, contudo, que quem foi lesado, porém, leve dias até perceber o rombo deixado pelos estelionatários. Entre os boletins de ocorrência, 91,4% não têm horário do crime apontado e outros 4% indicam "em período incerto."

Em qualquer caso de golpe, as autoridades recomendam o registro de boletim de ocorrência.

Além dos clássicos estelionatos eletrônicos, as legislações de delitos digitais incluem casos de falsificação de cartões e documentos.

No país, são duas leis que tipificam os delitos digitais: a Lei de Crimes Cibernéticos, mais conhecida como Lei Caroline Dieckmann; e, a lei 14.155 de 2021, que prevê o crime de invasão de dispositivo informático.

É crime digital:

- > invadir dispositivo informático;
 - > comercializar informações vazadas;
 - > interrupção de serviço telefônico, informático ou de informação de utilidade pública;
 - > falsificar documento;
 - > falsificar cartão;
 - > cometer estelionato por meio de dispositivo eletrônico com ou sem violação de mecanismo de segurança, utilização de programa malicioso ou outro meio fraudulento.
- > São agravantes visar idosos e vulneráveis e operações internacionais, como no caso das redes de cibercriminosos que ultrapassam fronteiras.

Veículo: Impresso -> Jornal -> Jornal da Cidade - Bauru/SP

Pagina: 30