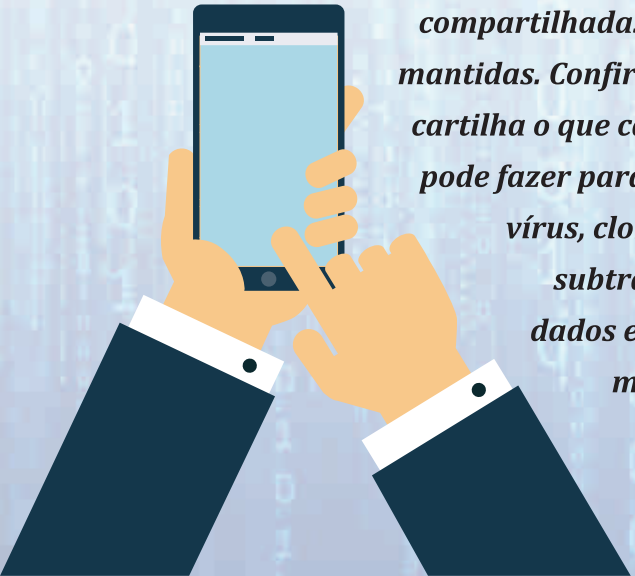
Diretrizes básicas para segurança no uso dos celulares

PJERJ

PODER JUDICIÁRIO
ESTADO DO RIO DE JANEIRO

Algumas dicas de segurança básica no uso de aparelhos celulares são aqui sugeridas pelo Comitê Gestor de Segurança da Informação (CGSI) do Tribunal de Justiça do Estado do Rio de Janeiro. Os recursos digitais são indispensáveis em nosso dia a dia, mas alguns cuidados são essenciais para que a confidencialidade e a integridade das informações compartilhadas sejam mantidas. Confira nesta cartilha o que cada um pode fazer para evitar vírus, clonagem, subtração de dados e outros males do século XXI.



I - SENHAS E BLOQUEIO

- Coloque uma senha em seu smartphone e em dispositivos (tablets e computadores)
- Use uma senha diferente para cada serviço e site
- Proteja a conta Google e o Apple ID com autenticação em dois fatores
- Evite senhas simples ou com informações pessoais (time de futebol favorito etc). Prefira senhas que tenham caracteres maiúsculos, minúsculos, caracteres especiais (@#$%_) e números
- Não anote senhas em post it ou em papéis que fiquem expostos
- Alguns softwares possuem gerenciador de senhas
- É recomendável a criação de uma senha de usuário no computador. Para evitar o acesso às configurações desse equipamento, é necessário que a navegação seja feita com o login de usuário e não como administrador (Admin)
- Também é recomendável o uso de criptografia e senha em pen drives

II - SMARTPHONES

- Procure anotar o IMEI do seu smartphone. O número pode ser obtido na nota fiscal do produto, na caixa do aparelho ou na plataforma disponibilizada pelo fabricante. Também é possível obtê-lo digitando *#06# no teclado

- Instale somente aplicativos da loja oficial e evite instalar sistemas que permitem o uso de programas piratas e não reconhecidos pelas lojas (root)

- Mantenha o sistema operacional e os aplicativos atualizados, de preferência habilitando a atualização automática

- Configure um bloqueio para a tela do celular

- Cuidado ao compartilhar códigos recebidos por SMS

- Ao usar os aplicativos de mensagem, como WhatsApp e Telegram, utilize a proteção de autenticação de dois fatores e desative o backup em nuvem

- Verifique e controle os aparelhos com sessões ativas do WhatsApp web

- Evite deixar que outras pessoas usem o seu telefone celular

- Apague os dados do seu aparelho se ele for subtraído ou extraviado

III - REDES E CONEXÕES

- Evite o uso de redes wi-fi públicas (bares e aeroportos), e tome cuidado com a conexão em hotéis
- Habilite o wi-fi apenas durante o período de uso. Não se esqueça de desligá-lo ao término do trabalho para que seu aparelho não se conecte a redes públicas automaticamente
- Ative o bluetooth dos dispositivos apenas quando for utilizar alguma aplicação
- Instale um antivírus em computador, tablet e smartphone. No computador, tenha também um detector de spyware (software espião de computador para observação e subtração de informações pessoais)
- Evite usar nome próprio em wi-fi do smartphone. Alguns softwares coletam nomes de rede
- Oculte o nome da sua rede sem fio residencial (Service Set Identifier/SSID)
- Não clique em links desconhecidos, especialmente aqueles em encurtadores de URLs, como o bit.ly
- Ao acessar sites ou ambientes suspeitos, use VPN, uma forma anônima de navegação que cria um computador virtual que é apagado após o uso, evitando boa parte das contaminações por vírus

IV - PHISHING

- Se houver dúvida em relação ao envio do link, procure confirmar a veracidade da mensagem com a empresa ou instituição remetente. Ex: intimações da Receita Federal, da Polícia Civil, de tribunais etc

- Ao passar o cursor em cima de um link suspeito, é possível verificar o real endereço no canto esquerdo inferior da janela, conferindo se corresponde ao link apresentado

V - COMPRAS NA INTERNET

- Alguns sistemas de pagamento on-line, como o PayPal, concentram as informações de cartões bancários, não sendo necessário divulgar tais dados em todos os sites em que você fizer compras, restringindo o acesso e minimizando a possibilidade de fraudes

- Se possível, ative o recurso de comunicação de gastos do cartão através de mensagens SMS. Tal recurso permite um maior controle e viabiliza a identificação imediata de uma compra não realizada. Se você identificar uma compra fraudulenta, comunique imediatamente a instituição financeira e não reconheça o gasto

VI - OUTROS CUIDADOS

- Faça backups de seus arquivos essenciais regularmente, de preferência, em um hd externo
- Não forneça dados pessoais por telefone
- Evite atender telefone com número restrito
- Restrinja a divulgação do seu número de telefone
- Caso suspeite da ligação recebida no telefone fixo de sua casa, nunca se identifique como dono do imóvel. Diga que é o empregado e desligue
- Evite atender ligações a cobrar. Não ceda a pedidos de cartões telefônicos ou de depósitos bancários
- Em caso de ameaças anônimas, mantenha a calma e tente conseguir o máximo de informações
- Instale aplicativos de reconhecimento de telefones, como o TrueCaller, que é gratuito, identifica números desconhecidos e bloqueia chamadas indesejadas
- Oriente seus familiares e servidores a não fornecerem dados pessoais por telefone
- Nunca se identifique primeiro ao receber uma chamada
- Evite colocar na agenda telefônica do celular dados que possam identificar pessoas muito próximas, principalmente familiares. Exemplo: pai, mãe, esposa, filho etc
- Instale em seu telefone fixo um sistema identificador de chamadas
- Não divulgue a sua rotina em redes sociais

- Observe as orientações para uso de redes sociais que constam no “Manual da AMB para magistrados - o uso das redes sociais”, cujo link está disponibilizado no final desta cartilha

- Cuidado com o descarte de lixo. Vide o War Trashing https://www.youtube.com/watch?v=tbAPZSdOvSs

- Uso de serviços eletrônicos na área do transporte privado urbano (Uber, 99 Táxi etc) – Facça um print screen (captura de tela) da identificação do motorista e placa do veículo, e, se possível, encaminhe-o para uma pessoa de confiança. Procure compartilhar a viagem em tempo real com alguém de confiança

- Roubo de iPhone – É comum, após roubo ou furto de iPhone, o envio de um SMS comunicando suposta recuperação do aparelho. Trata-se de um falso link que visa obter o login do usuário para desbloqueio do aparelho. Não clique nesse link, nem preencha formulários que solicitem senha

- O recurso de compartilhamento da localização em tempo real é disponibilizado por alguns aplicativos e pode ser utilizado como medida de segurança

- Trate a rede social como um ambiente público. Não se deixe levar pela falsa sensação de privacidade que, eventualmente, ela possa transmitir

- Cuidado com contatos de estranhos na sua rede de relacionamentos digitais, por mais que pareçam amigos. Perfis de redes sociais são facilmente manipulados para obtenção de informações

- Alguns programas e aplicativos permitem a configuração das opções de privacidade

- Não divulgue dados pessoais! Nomes, sobrenomes, telefones e endereços são informações frequentemente usadas por marginais para a prática de golpes e ilícitos contra o usuário da rede social e/ou de seus familiares

- Cuidado com as imagens publicadas na rede! As fotografias "falam" e revelam detalhes da nossa vida que podem chamar a atenção de criminosos ou mesmo contribuir para a prática de delitos. Endereço residencial, rotinas, locais frequentados, profissão exercida, dados sobre familiares e destinos de viagens são algumas informações que podem ser captadas através de fotografias

- Check-in é o ato de compartilhar a localização em redes sociais. Essa prática não é recomendada, uma vez que expõe demasiadamente a vida da pessoa. O check-in indica, em tempo real, os lugares frequentados pelo usuário, sendo possível delinear o seu perfil e sua rotina. Por outro lado, também pode sinalizar a ausência de alguém, informação útil para furtos a residências

- E lembre-se do provérbio que diz "Há três coisas na vida que nunca voltam atrás: a flecha lançada, a palavra pronunciada e a oportunidade perdida". O conteúdo digital gerado no celular tornou-se a quarta.

FONTES

http://www.cnj.jus.br/files/conteudo/arquivo/2017/09/e3e89ee45236107bcfcb1ea810826b16.pdf

http://www.amb.com.br/wp-content/uploads/2017/07/Manual-da-AMB-para-magistrados_-o-uso-das-redes-sociais_SITE_v2.pdf

http://www.amb.com.br/wp-content/uploads/2017/04/0151246.pdf

https://g1.globo.com/economia/tecnologia/noticia/2019/06/12/saiba-aumentar-a-seguranca-do-celular-e-dos-aplicativos-de-mensagens.ghtml

http://www.coaliza.org.br/wp-content/uploads/2014/05/Cartilha-TJERJ.pdf

PJERJ

PODER JUDICIÁRIO
ESTADO DO RIO DE JANEIRO

Des. Claudio de Mello Tavares
Presidente do Tribunal de Justiça

Des. Bernardo Moreira Garcez Neto
Corregedor-Geral da Justiça

Des. Reinaldo Pinto Alberto Filho
1º Vice-Presidente

Des. Paulo de Tarso Neves
2º Vice-Presidente

Des. Elisabete Filizzola Assunção
3ª Vice-Presidente

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)

Des. Nagib Slaibi Filho
Presidente

Des. Luciano Silva Barreto

Juiz Fabio Ribeiro Porto

Juiz Leandro Loyola de Abreu

Juiz Gustavo Quintanilha Telles de Menezes

Juiz Wilson Marcelo Kozlowski Júnior

Juiz Anderson de Paiva Gabriel

DIRETORIAS-GERAIS

Humberto Vieira da Cruz
Diretor-Geral de Tecnologia da Informação e Comunicação de Dados (DGTEC)

Francisco Costa Matias de Carvalho
Diretor-Geral de Segurança Institucional (DGSEI)

Solange Rezende Carvalho Duarte
Diretora-Geral de Comunicação e de Difusão do Conhecimento (DGCOM)

MEMBROS DA ÁREA TÉCNICA

Ivan Lindenberg Junior
Especialista em Segurança da Informação

Wagner da Silva Andrade Junior
Especialista em Telecomunicações

Jorge Luiz Monteiro Rodrigues
Especialista em Segurança Física

Raquel Rocha de Oliveira
Especialista em Comunicação

MEMBROS DA ÁREA INSTITUCIONAL E JURISDICIONAL

Alessandra Fabrício Anátocles da Silva Ferreira
Diretora-Geral de Apoio aos Órgãos Jurisdicionais (DGJUR)

Michele Vieira de Oliveira
Representante da área de Gestão Estratégica e de Planejamento

Debora Ferreira de Sousa
Representante da Corregedoria Geral da Justiça