COVID-19

E

SEGURANÇA DIGITAL

ORDEM DOS ADVOGADOS
SEÇÃO DE SÃO PAULO

CAIO AUGUSTO SILVA DOS SANTO
PRESIDENTE OAB SP

RICARDO TOLEDO SANTOS FILHO
VICE- PRESIDENTE OAB SP

SPENCER TOTH SYDOW
PRESIDENTE DA COMISSÃO ESPECIAL DE DIREITO DIGITAL

CHRISTIANY PEGORARI CONTE
VICE-PRESIDENTE DA COMISSÃO DE ESPECIAL DE DIREITO DIGITAL

ORLANDO CARVALHO SBRANA
MEMBRO COLABORADOR

SUMÁRIO

APRESENTAÇÃO

Prezados Colegas,

A presente cartilha foi elaborada pela Comissão de Direito Digital, na qual trata das questões sobre a COVID-19 e a Segurança Digital, informa sobre os riscos digitais que existem ao nosso redor bem como os modos de evitá-los.

A OAB SP, assim, contribuem para disponibilizar ao público o referido conteúdo no site, bem como na página da Comissão de Direito Digital.

São Paulo, 08 de abril de 2020.

DIRETORIA DA SECIONAL

Presidente
Caio Augusto Silva dos Santos

Vice-Presidente
Ricardo Toledo Santos Filho

Secretário-Geral
Aislan de Queiroga Trigo

Secretária-Geral Adjunta
Margarete de Cássia Lopes

Diretora Tesoureira
Raquel Elita Alves Preto

DIRETORIA DA COMISSÃO

Presidente
Spencer Toth Sydow

Vice-Presidente
Christiany Pegorari Conte

Secretaria-Geral
Katia Shimizu de Castro

INTRODUÇÃO:

Em tempos de incertezas e dificuldades geradas por uma situação de calamidade pública na área da saúde pública e que nos impõem medidas radicais, é importante que saibamos dos riscos digitais que existem ao nosso redor bem como os modos de evitá-los.

A criminalidade aproveita de situações especiais e cria novos golpes, as fake news se disseminam descontroladamente em um ciclo perigoso de desinformação e a situação de isolamento nos obriga a fazer nossos trabalhos a partir de nossas casas (home office).

A OAB-SP, através de sua Comissão de Direito Digital, preocupada com o cenário enfrentado, identificando as dificuldades do lido com as novas situações impostas e o crescimento de inseguranças, decidiu elaborar um rápido manual para auxiliar advogados e demais profissionais nas três áreas apontadas.

Esperamos poder ajudar!

CUIDADOS COM AS FAKE NEWS:

As pessoas estão muito preocupadas com a situação mundial. Disso não há a menor dúvida. Por conta dessa preocupação, muito se tem dito e escrito sobre o tema.

A virtualidade, porém, não difere o que foi escrito com base científica, por especialistas e o que é simplesmente opinião pessoal de pessoas sem respaldo. Em verdade, sempre há muita coisa errada sendo dita.

Como todos temos direito constitucional de nos expressar livremente, sempre haverá opiniões e rumores sendo propagados por pessoas. Contudo, temos que diferenciar um rumor de uma fake news.

Uma coisa é emitir uma opinião própria. Outra coisa é repetir e propagar opiniões alheias sem verificar suas bases e fundamentos. É desse mal que sofre a sociedade hoje: disseminação descontrolada de informações erradas que podem gerar desde medo, a golpes e a problemas sociais.

Excesso de curiosidade gera excesso de informação. E todos queremos ser os emissários das novidades. Mas isso precisa ser feito com parcimônia, especialmente por advogados.

Nossas opiniões são respeitadas. Somos formadores de opinião.

Em tempos de pandemia, o que mais ocorre são informações erradas que ajudam empresas aproveitadoras a terem lucro, que geram ações indevidas e que prejudicam o próprio combate à doença.

Dentre alguns dos absurdos propagados estão (i) Beber água a cada 15 minutos para combater o vírus, (ii) Beber água quente para matar o vírus e até que (iii) Álcool gel não serve para assepsia.

Essas informações estão todas erradas.

São tantas as fake news que envolvem o CORONAVÍRUS, que o Ministério da Saúde colocou em seu site uma página dedicada apenas a combater tais informações erradas propagadas.

Assim, para que evitemos que as fake news se espalhem, devemos fazer exatamente como estamos fazendo na questão do isolamento social: precisamos nos retirar da cadeia de disseminação, impedindo a multiplicação das informações falsas e erradas.

Para que apenas compartilhemos informações CORRETAS, eis alguns cuidados que devemos tomar:

1) Buscar a fonte da notícia. Notícias sem fonte não devem NUNCA ser compartilhadas e disseminadas. Não importa se está escrito na informação que "quem disse foi o Jabor", que "deu certo na Alemanha" que a "ciência já comprovou" ou "ninguém quer que isso se espalhe". Busque ter certeza antes de compartilhar.

2) Se está com dificuldades de identificar a fonte, utilize de sites especializados em desmascarar fake news. Alguns exemplos são os sites "Fato ou Fake", "Comprova", "Agência Pública", "Boatos", "Aos Fatos" e "farsas".

3) Esses sites acima inclusive recebem denúncias de Fake News. Se você identificar uma, por favor, denuncie.

4) Instituições sólidas como a OAB, bancos, Governos e marcas multinacionais não se utilizam de mensagens de email ou SMS para se comunicarem com o público. Busque diretamente o site da empresa, sempre que se atribuir a notícia a alguma instituição.

5) Não compartilhe pedidos de ajuda de que não conhece a origem. Pode ser golpe.

6) Não use redes sociais ou grupos para propagar conteúdo alheio, ou de origem duvidosa. Você está multiplicando em muitas vezes o potencial de alastramento.

ATENÇÃO AOS GOLPES:

Os delinquentes não se importam com o delicado estado das pessoas que, por conta do afastamento do trabalho, enfrentam dificuldades financeiras e para pagamento de suas contas.

Em verdade, são as situações de desastre e comoção social que geram o pretexto normalmente utilizado pela criminalidade para a aplicação de golpes que visam prejuízo patrimonial e obtenção de dados.

O surgimento da pandemia do COVID-19 gera medo, precaução e cuidados especiais nos Estados e nos cidadão. Isso traz consigo expressões próprias e gera curiosidades nas pessoas, como demonstrado no capítulo anterior.

Aproveitando-se do interesse especial gerado, delinquentes fazem uso da denominada "engenhosidade social" para criar métodos de atração e armadilhas de modo a fazer com que usuários cliquem em links, preencham formulários, cedam informações sensíveis e façam pagamentos indevidos sob falsos pretextos.

Também, o fato de as pessoas terem maior tempo disponível em casa e aumentarem o uso de dispositivos informáticos faz com que golpes antigos sejam intensificados.

Fiquem atentos aos principais golpes existentes neste momento.

1 - O ‘’Corona Voucher":

O Governo Brasileiro publicou pelo Diário Nacional, o programa de auxílio emergencial que pagará até R$ 600 para cidadãos que tiveram suas economias atingidas pela crise do coronavírus. Os delinquentes enviam mensagens por SMS, WhatsApp e /ou e-mail sugerindo que o usuário interessado em pleitear o benefício clique em links que o direcionam a sites espelho que se assemelham a site oficial do Governo Federal para preencherem um falso cadastro.

Ali, dados sensíveis são cedidos ou números de cartão de crédito são fornecidos.

Se você tiver direito ao auxílio, NINGUÉM entrará em contato com você. Cabe a você a iniciativa de buscar o auxílio através do meio adequado informado pelo governo (aplicativo ou site).

2 ‘COVID-19 Tracker’:

Criminosos informáticos aproveitando-se do medo motivado pela pandemia, criaram um falso aplicativo denominado ‘COVID-19 Tracker’ que supostamente fornece dados sobre o coronavírus no mundo. Quando o aplicativo é instalado há a obtenção de dados sensíveis da vítima como senhas e números de cartão de crédito e consegue-se controle remoto dos dispositivos.

Apesar de existirem programas que realmente fazem isso, é preciso pesquisar quais aplicativos são confiáveis antes de instalá-los. Sugerimos que o acompanhamento seja feito via sites oficiais e não aplicativos, especialmente porque a Lei Geral de Proteção de Dados ainda não se encontra em vigor.

3. Falso site da Ambev/ Doação de Álcool Gel:

Aproveitando-se da credibilidade da empresa que manifestou-se no sentido de auxiliar na produção de álcool gel, mensagens falsas oferecendo o produto gratuitamente foram disparadas mediante cadastramento. O usuário cadastra-se e fornece dados que serão utilizados indevidamente pelos delinquentes.

Não existe a situação em que uma empresa lhe procura para oferecer algo gratuitamente. Se houver uma distribuição de álcool gel isso certamente não ocorrerá através de uma mensagem que lhe oferece o auxílio via celular ou email.

4. “Hospital na China em sete dias”:

Mensagens sugerem que o usuário clique eu um link para baixar o vídeo que mostraria a construção de um hospital na China em sete dias. Não há qualquer vídeo. Trata-se de um malware que danifica o dispositivo e pode se apropriar de dados pessoais das vítimas.

Nunca acredite em mensagens com anexos não solicitados. Nunca acredite em anexos que propagam uma mídia em momentos de crise. Se houver interesse em assistir um vídeo, vá aos sites especializados.

5- Vacinação contra Coronavírus:

Neste golpe uma mensagem informa que existiria um cadastro prioritário de vacinação para pessoas que pagarem antecipadamente uma taxa. Um link direciona a vítima

para um site falso do Ministério da Saúde em que ela preenche dados e faz um pagamento via cartão de crédito ou boleto.

Não há um cadastro para vacinação oficial e o Governo Federal não poderia cobrar para discriminar pessoas a partir de condições econômicas. Quando houver vacinação toda a mídia irá propagar isso e campanhas ocorrerão.

6- Descoberta da cura da Pandemia:

Sob pretexto de uma notícia que fala sobre a cura do vírus, o usuário é instado a clicar em um link e, ali, instala-se um malware no dispositivo da pessoa que pode obter dados ou o controle remoto do aparelho.

Quando houver a cura, todos os canais de mídia a propagaram e não mensagens direcionadas.

7- Recadastramento de bancos:

Os criminosos enviam SMS e mensagens fazendo-se passar pelos principais bancos do país e informando que a pandemia os obriga a confirmar todos os dados do correntista. O usuário é levado ao site para colocar todos os dados bancários e do cartão de crédito.

Bancos NUNCA fazem recadastramento a partir de links e NUNCA pedem dados dessas naturezas.

8 - Confirmação de número de SMS:

Um telefonema é recebido e uma pessoa se identifica como organizador de algum evento pós pandemia como uma festa, um lançamento imobiliário ou sorteio. O interlocutor informa que para participar é preciso informar um código de 6 números que será recebido por SMS. Quando a pessoa recebe a mensagem e confirma os números seu WhatsApp

passa a ser controlado pelo delinquente que, então, dispara pedidos de ajuda financeira para a lista de contatos.

Nunca forneça os números enviados por SMS a NINGUÉM.

HOME OFFICE E SEGURANÇA DIGITAL:

A previsão legal do home office encontra-se definida nos artigos 75-A à 75-E da CLT, com a denominação de “teletrabalho”. Em verdade, o que fez a legislação foi regulamentar o trabalho à distância, que nos dias atuais foi facilitado pelo implemento da tecnologia.

A proteção de dados no trabalho remoto também já foi regulamentada pela Lei nº 13.709/18 (Lei Geral de Proteção de Dados). Em síntese o dispositivo normatiza o tratamento de dados pessoais. Assim sendo, no trabalho em home office, será ela que resguardará colaboradores, corporações e terceiros que tenham seus dados manejados à distância.

No trabalho em home office, uma das maiores preocupações dos empresários é a falta ou o menor controle de suas informações, pois, remotamente, a fiscalização dos dados pode ficar mais fragilizada, facilitando perdas, modificações, desvios ou até mesmo apropriações indevidas.

Por outro lado, o risco da elevação abrupta do número de pessoas contagiadas pelo novo Coronavírus, fez surgir uma necessidade premente de alteração do ambiente cotidiano de trabalho nas empresas, para aquele exercido em home office, evitando-se, com isso, aglomerações e difusão da pandemia.

Por muito tempo desacreditado e até as vezes repudiado, diante da pandemia as empresas se apegaram ao home office para dar continuidade às suas atividades.

Dessa necessidade, algumas percepções vantajosas puderam ser observadas:

- O tempo otimizado pelo colaborador é um dos principais benefícios, pois com ele evita-se deslocamento e permite um melhor gerenciamento da jornada de trabalho.

- Economia para as duas pontas, empresário e colaborador.

- Elevação da qualidade de vida dos trabalhadores.

Somando-se os prós e os contras, em tempos de COVID-19, uma coisa não se pode negar: existem vários riscos relativos à segurança digital no trabalho realizado por essa modalidade.

Entretanto, se alguns cuidados forem observados, o percentual de ocorrências negativas pode ser bastante reduzido.

Cuidados com o material de trabalho:

- Tenha sempre um bom antivírus instalado no seu dispositivo e atualize-o sempre.
- É recomendável que os dispositivos utilizados para trabalhos confidenciais sejam criptografados. Na impossibilidade, criptografe ao menos os dados e arquivos mais importantes.
- Realize cópias de segurança (backups) periódicos de seus dispositivos ou arquivos. Backups realizados em nuvem, atualmente vêm se mostrando cada vez mais seguros, pois são criptografados e contam com segurança em camadas.
- Opte, sempre que possível, pela autenticação de dois fatores em seus dispositivos. A autenticação de dois fatores é um recurso oferecido por vários prestadores de serviços online que acrescentam uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.

- Evite utilizar o equipamento de trabalho para atividades pessoais: lembre-se que na maioria das vezes dispositivos de trabalho são monitorados.

- Não faça download de softwares de origem duvidosa ou aplicativos “piratas".

- Não abra e-mails de pessoas que você nunca estabeleceu contato anteriormente. Não faça downloads de arquivos anexos que não reconhece como pertinentes àquela troca de mensagens.

- Cuidado ao usar um computador compartilhado, essa prática multiplica os riscos de expor suas senhas e arquivos confidenciais. Caso seja necessário usar um computador que outros também utilizarão, não salve senhas em programas ou navegadores.

- Evite navegar por sites desconhecidos ou de conteúdo suspeito, páginas mal-intencionadas podem conter vírus ou malware, danificando seu dispositivo de trabalho. Estatísticas do Google mostram que a empresa costuma encontrar cerca de 9,5 mil novos sites maliciosos por dia no seu buscador.

- Evite que familiares e amigos utilizem o dispositivo do trabalho para evitar navegações indevidas e incidentes de segurança.

<u>Cuidados com a rede:</u>

- Utilize conexão segura sempre que a comunicação envolver dados confidenciais. Dê preferência àquelas redes que oferecem autenticação e são criptografadas.

- Redes Wi-Fi por se conectarem por meio de sinais de rádio, não necessitam de acesso físico a um ambiente privativo, como ocorre com as redes cabeadas.

Diante disto, os dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento, como por exemplo um notebook.

- Caso faça videoconferência, opte por utilizar um programa com encriptação em ambas as pontas.

- Não utilize redes desconhecidas para fins laborais.

Cuidados com você:

- Lembre-se de fazer pausas a cada 40 ou 50 minutos. Desvie o olhar da tela, estique as pernas e vá dar uma volta.

- Não tenha alimentos a disposição no local de trabalho. Quando tiver fome levante-se, espaireça e vá até a cozinha. Não coma alimentos muito gordurosos e doces para não ter sono e para não descuidar da saúde.

- Não tenha bebida alcoólica próxima nos momentos de trabalho.

- Não deixe abas abertas com assuntos que distraiam. É momento de trabalho e não de lazer.

- Mantenha o celular distante ou no silencioso para não perder o foco.

- Acorde na mesma hora de sempre. Crie uma rotina. Afinal, é home office e não feriado.

- Peça que durante seu período de trabalho seja feito silêncio em seu local de trabalho e que todos respeitem esse momento

CANAIS DE APOIO:

- www.oabsp.org.br
- https://www.saude.gov.br/fakenews
- https://www.e-farsas.com/
- https://apublica.org/checagem/
- https://projetocomprova.com.br/
- https://g1.globo.com/fato-ou-fake/
- https://aosfatos.org/
- https://www.boatos.org/