COVID-19, segurança de informação e privacidade

Abril de 2020 (versão 1.1)

Uma brochura PFC Consulting para a sua empresa

PFC CONSULTING

https://www.pfcconsulting.pt

Introdução

As circunstâncias atuais conduziram a uma mudança de hábitos por parte das empresas e dos particulares, incluindo:

- Uma maior procura de bens, sobretudo os de proteção individual e farmacêuticos;
- Uma descida na mobilidade;
- Maior permanência nas habitações e um aumento significativo do teletrabalho, dependendo de soluções digitais;
- Limitações da vida pública, que tornam as atividades criminosas menos visíveis e movendo-as para outros vetores, como a casa e a vida digital;
- Aumento da ansiedade e do medo, propício para criar vulnerabilidades e para melhor explorar essas vulnerabilidades;
- Decréscimo de bens ilícitos no mercado tradicional.

Estas mudanças conduzem a um aumento significativo da criminalidade, sobretudo a que diz respeito a:

- Cibercrime;
- Fraude;
- Fabrico e distribuição de produtos contrafeitos e/ou de qualidade inferior;
- Crime organizado.

O objetivo desta brochura é o de dar algumas dicas aos colaboradores sobre como podem proteger-se para minimizar a probabilidade de ser alvo desta criminalidade.

Teletrabalho

A empresa encoraja-o, neste período excecional, a trabalhar de casa, aumentando a sua flexibilidade. Porém, se não acautelar a segurança e privacidade, pode expor-se a si e à sua empresa a vulnerabilidades que podem conduzir a consequências graves.

Utilize apenas equipamento e software fornecido pela empresa;

Se não tiver possibilidade de utilizar equipamento e software fornecido pela empresa:

- Mantenha as suas aplicações e sistema operativo atualizados;
- Utilize software antimalware e mantenha-o atualizado;
- Conecte-se à sua empresa apenas através de uma VPN aprovada.

Configure corretamente a sua aplicação de vídeo conferência e atualize-a logo que haja atualizações disponíveis.

Não utilize o equipamento e software da empresa para atividades de lazer;

Não partilhe o equipamento utilizado em teletrabalho com a sua família e amigos. Se não houver alternativa, utilize contas separadas. Não partilhe, sob nenhuma circunstância, as suas passwords. Nunca abandone o equipamento nem o utilize em locais públicos. Bloqueie sempre o ecrã.

Não partilhe informações pessoais.

Adapte as suas rotinas, incluindo as que dizem respeito à alocação de tarefas, ao cumprimento de objetivos e à comunicação.

Mantenha-se alerta e reporte situações que lhe pareçam suspeitas.

Phishing, Smishing e Vishing

Embora sejam termos estranhos, eles são apenas os nomes que são dados às técnicas de engenharia social utilizadas para o enganar e o levar a fazer uma ação que de outro modo não faria, por exemplo clicar num link, descarregar um programa ou fazer uma transferência bancária. O phishing por e-mail, o smishing por SMS e o vishing por voz.

Não clique em links, anexos ou imagens que tenha recebido em email ou SMS não solicitados sem que primeiro valide o remetente.

Não se apresse a responder. Analise a mensagem com calma antes de responder.

Não responda a mensagem em que lhe solicitem um PIN, usernames e passwords ou outro tipo de credenciais de acesso.

Preste atenção a chamadas recebidas não solicitadas. Fique com o número, procure se o número é fiável (por exemplo se pertence à sua empresa) e ligue de volta apenas se confirmar a validade.

Não efetue operações, por exemplo uma transferência bancária, se não seguir o circuito habitual de aprovações e validações.

COMO FUNCIONA?

Tipicamente é enviada uma mensagem muito semelhante a uma mensagem de um remetente real. Há alguns sinais, porém, que podem denunciar tal mensagem como ilegítima:

- a existência de erros ortográficos ou de sintaxe;
- uma linguagem que transmite uma sensação de algo urgente;
- um link, imagem ou anexo associados;
- um remetente ou um apontador de um link que não corresponde a um destinatário conhecido;
- uma oferta boa demais para ser verdade;
- a solicitação de dados pessoais ou de acesso.

Compras online e outros cuidados

Os criminosos aproveitam esta circunstância para publicarem anúncios falsos de produtos que queremos e precisamos, como medicamentos, vacinas, produtos de higiene e kits de teste.

Se algo lhe parece bom demais para ser verdade, é porque é provavelmente falso.

Faça compras online apenas em vendedores cuja reputação é sólida ou cujos ratings são elevados.

Utilize o cartão de crédito apenas em sites que comecem com https. Se possível, use cartões virtuais.

Quando a venda é feita cliente a cliente, não pague primeiro para ter o produto depois.

Se um produto estiver esgotado em todo o lado, desconfie de um fornecedor que tenha o produto disponível.

Não faça donativos para causas que não estão suficientemente alicerçadas e onde possa, sem margem para dúvida, conhecer a autenticidade.

Não siga indicações de estranhos para fazer pagamentos com MBWay. Embora este seja um meio de pagamento recomendado nestas circunstâncias, seja cuidadoso.

Não confie nem partilhe notícias que não provenham de fontes oficiais e de sólida reputação. Sobre o COVID-19, confie apenas nos sites associados ao Ministério da Saúde, à Organização Mundial de Saúde e da Organização das Nações Unidas.

Reveja as permissões associadas às aplicações que tiver em telemóveis, tablets ou telemóveis.

Reveja as configurações de privacidade associadas às suas contas de redes sociais.

Proteja as crianças. Vigie os seus hábitos online e utilize uma aplicação de controlo parental.

Em caso de dúvida ou questão sobre segurança de informação contacte a área de segurança da sua empresa ou a sua chefia.