MANUAL DE BOAS PRÁTICAS E SEGURANÇA DA INFORMAÇÃO

Aqui vamos conferir algumas dicas que ajudarão a utilizar os recursos do órgão, conforme políticas aprovadas, e orientações de como identificar ataques que podem expor os dados a pessoas de fora da organização.

1. DICAS GERAIS DE SEGURANÇA

- Não baixe aplicativos desconhecidos ou de origem duvidosa;
- Utilize a verificação em duas etapas (2FA) em todas as plataformas e contas possíveis;
- Sempre use conexões seguras, certificando-se da presença do protocolo "https://" para o acesso aos sites;
- Mantenha sempre os seus aplicativos e sistemas atualizados, principalmente o Windows e o antivírus;
- Ao se ausentar do seu posto de trabalho ou equipamento de informática, realize imediatamente o bloqueio de tela;
- No transporte de dispositivos móveis, mantenha-os protegidos contra o acesso visual ou físico de terceiros.

2. GESTÃO E COMPLEXIDADE DE SENHAS

- Evite senhas de baixa complexidade, termos sequenciais ou combinações óbvias;
- Evite a utilização de datas de nascimento, números de telefone, nome da empresa ou quaisquer dados pessoais de fácil acesso público;
- Crie senhas robustas contendo, no mínimo, 8 caracteres;
- Inclua obrigatoriamente ao menos 1 caractere especial (ex: @, #, $, &) e 1 letra maiúscula na composição.

3. E-MAIL, SPAM E ENGENHARIA REVERSA (PHISHING)

O Phishing é uma técnica de engenharia social estruturada para engenhar usuários legítimos e obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartões de crédito corporativos ou pessoais. Para cometer fraudes eletrônicas, os criminosos utilizam mensagens com identidade visual perfeitamente clonada, simulando a comunicação de grandes empresas ou instituições públicas.

- Nunca abra arquivos anexos de e-mails de origens desconhecidas ou não solicitadas;
- Analise cuidadosamente os e-mails com anexos, mesmo quando enviados por pessoas ou contatos conhecidos (o remetente pode ter sido clonado);
- Não efetue o preenchimento de cadastros ou formulários de pesquisas enviados anexos ao corpo da mensagem;
- Atente-se redobradamente ao abrir e-mails supostamente enviados por instituições bancárias oficiais e órgãos da administração pública;
- Ao clicar em links recebidos, confirme na barra de endereços do navegador o domínio real. Existem muitos links falsos que direcionam para páginas clonadas com fins fraudulentos.

4. COMO IDENTIFICAR UM E-MAIL FALSO?

Fique alerta e observe a presença constante de um ou mais dos seguintes indicadores:

1. O remetente do e-mail possui um endereço estranho ou desprovido de domínio oficial corporativo;

2. A mensagem promete vantagens excessivas, ganhos fáceis ou rápidos, sem contrapartida lógica;

3. O e-mail solicita explicitamente o preenchimento de dados cadastrais ou informações financeiras;

4. Há presença de boletos, faturas ou notas fiscais anexas de serviços nunca contratados;

5. As informações textuais apresentam-se desencontradas, confusas ou com sérios erros de concordância;

6. Uso ostensivo de senso de urgência ou ameaças veladas (ex: 'Sua conta expira hoje', 'Evite multa imediata');

7. Erros graves de ortografia, acentuação ou desleixo evidente na formatação geral;

8. O endereço do remetente exibido e o endereço configurado para resposta (reply-to) são divergentes;

9. Apresentação de uma proposta comercial ou benefício absurdamente incompatível com as práticas de mercado.

5. ENGENHARIA SOCIAL E ARMADILHAS COTIDIANAS

A engenharia social compreende a manipulação psicológica do indivíduo para explorar o elo mais sensível da segurança. Utilizam-se técnicas comportamentais para despertar gatilhos como curiosidade, culpa, solidariedade cega e medo, garantindo o acesso facilitado aos dados sensíveis de pessoas e empresas.

> **MÁXIMA ATENÇÃO COM E-MAILS OU MENSAGENS CONTENDO:**
> • *"Clique aqui e veja nossas fotos"*
> • *"Seu nome foi incluído no SERASA – Clique aqui para saber o motivo"*
> • *"Atualize seu token corporativo por e-mail"*
>
> *Lembre-se: fraudes também ocorrem por chamadas telefônicas (falsos sequestros, suporte técnico falso) ou SMS (falsas promoções de programas de TV). Atente-se constantemente, pois novas armadilhas surgem diariamente!*

6. DIRETRIZES PARA A PROTEÇÃO DE DADOS E PRIVACIDADE

Paralelamente aos investimentos em segurança e infraestrutura promovidos pelo órgão, cabe a cada servidor e colaborador zelar pela conformidade e proteção por meio das seguintes práticas de privacidade:

6.1. Inspeção de Endereços Eletrônicos

Ao navegar, valide a autenticidade e o nível de segurança do ambiente digital. Certifique-se de que a página possui certificado válido assinado por uma autoridade reconhecida. Identifique o ícone do cadeado de segurança ao lado da URL, clicando sobre ele para verificar os dados de conexão.

6.2. Segregação e Exclusividade de Credenciais

A utilização de senhas idênticas para sistemas internos da empresa e e-mails pessoais eleva exponencialmente o risco sistêmico. Se uma credencial for exposta em um vazamento externo, o invasor tentará os mesmos dados nos

sistemas institucionais. Recomenda-se o uso de gerenciadores corporativos homologados para a custódia e geração de senhas aleatórias robustas.

6.3. Obrigatoriedade do Duplo Fator de Autenticação

A autenticação em múltiplos fatores (MFA) estabelece barreiras adicionais de verificação (senha combinada com token dinâmico ou biometria). Sua ativação mitiga consideravelmente o perigo do comprometimento de senhas estáticas.

6.4. Postura Defensiva com Ofertas Gratuitas

Adote o ceticismo profissional na rede: não existem brindes ou vantagens sem custo na internet. Sempre utilize uma conta de e-mail secundária, estritamente isolada do domínio institucional, para efetuar cadastros e assinaturas de serviços não oficiais.

6.5. Isolamento Físico de Periféricos de Áudio e Vídeo

Códigos maliciosos avançados podem habilitar remotamente microfones e webcams para espionagem corporativa. Desative as permissões no sistema operacional quando não estiver em videoconferências e use barreiras físicas (fitas ou protetores dedicados) para cobrir as lentes da câmera.

Estas diretrizes básicas protegem você e a instituição contra os principais vetores de ataques cibernéticos. Em caso de qualquer anomalia, comportamento suspeito ou dúvida, acione imediatamente o setor de Tecnologia da Informação (T.I.).