CARTILHA DE SEGURANÇA DIGITAL E PREVENÇÃO A FRAUDES ELETRÔNICAS

1. Contexto e Conformidade Normativa

A **Resolução CMN nº 4.893/2021** estabelece as diretrizes para a política de segurança cibernética e os requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Esta cartilha cumpre as diretrizes da norma no que tange à **disseminação da cultura de segurança cibernética**, ao **treinamento e conscientização de colaboradores** e ao **reforço dos controles de prevenção a incidentes e mitigação de vulnerabilidades**.

Os Três Pilares da Segurança da Informação (Art. 2º)

- **Confidencialidade:** Garantia de que informações sensíveis e dados cadastrais/financeiros só sejam acessados por pessoas autorizadas.
- **Integridade:** Preservação da exatidão e completidão dos dados, impedindo alterações não autorizadas.
- **Disponibilidade:** Garantia de que os sistemas e serviços estejam acessíveis e operacionais sempre que necessário.

2. Principais Ameaças Digitais e Técnicas de Ataque

A. Engenharia Social

É a manipulação psicológica de pessoas para que executem ações confidenciais, forneçam senhas ou concedam acesso a sistemas restritos. Explore gatilhos como **urgência**, **autoridade**, **curiosidade** e **medo**.

B. Phishing (E-mail e Web)

Ataque que utiliza comunicações falsas — simulando bancos, órgãos governamentais ou empresas de tecnologia — para induzir a vítima a clicar em links maliciosos ou baixar anexos infectados (*malware*).

- **Spear Phishing:** Phishing altamente direcionado a uma pessoa ou setor específico, com dados personalizados.
- **Whaling:** Phishing direcionado a executivos de alto escalão (*C-level*).

C. Smishing (SMS / Mensagens de Texto)

Tentativa de golpe realizada por meio de SMS ou aplicativos de mensagem (como WhatsApp e Telegram). O golpista envia links para páginas falsas alegando bloqueio de conta, milhas acumuladas ou compras não autorizadas.

D. Vishing (Phishing por Voz)

Chamadas telefônicas em que o atacante se passa por um funcionário da instituição financeira, central de segurança ou suporte técnico, solicitando senhas, códigos de validação (OTP) ou transferências de teste.

E. Outras Fraudes Eletrônicas Frequentes

- **Golpe do Falso Funcionário / Central de Atendimento:** O fraudador orienta a vítima a realizar procedimentos de "segurança" no aplicativo do banco que, na verdade, transferem valores.
- **SIM Swapping (Clonagem de CHIP):** Transferência não autorizada do número de telefone para outro CHIP de celular, permitindo ao criminoso interceptar SMS de verificação.
- **Malware Bancário / Keyloggers:** Softwares maliciosos instalados silenciosamente que capturam senhas digitadas ou espelham telas.

3. Matriz Comparativa de Ameaças

Canal	Tipo de Ataque	Vetor Principal	Objetivo Principal
E-mail	Phishing	Links falsos e anexos maliciosos (`.exe`, `.zip`)	Roubo de credenciais e infecção por malware
SMS / Mensageria	Smishing	Mensagens curtas com senso de urgência	Captura de tokens/OTP e cliques em sites falsos
Ligação Telefônica	Vishing	Manipulação verbal e falsificação de chamadas	Obtenção de senhas e realização de transferências
Redes Sociais	Engenharia Social	Perfis fakes, engenharia de relacionamento	Coleta de dados pessoais e golpes financeiros

4. Guia Rápido de Prevenção e Boas Práticas

1. **Desconfie do Senso de Urgência:** Instituições financeiras não exigem ações imediatas sob ameaça de bloqueio instantâneo de conta via e-mail ou SMS.
2. **Valide a Origem das Mensagens:** Verifique o endereço do remetente (fique atento a grafias parecidas, como `banc0.com.br`) e não utilize os números de telefone informados na própria mensagem suspeita.

3. **Nunca Compartilhe Credenciais ou Tokens:** Senhas, PINs e códigos de verificação em duas etapas (2FA) são **pessoais e intransferíveis**. Centrais legítimas jamais pedem esses dados.
4. **Cuidado com Links Reduzidos:** Evite clicar em links encurtados ou desconhecidos. Digite o endereço oficial da instituição diretamente no navegador.
5. **Autenticação em Dois Fatores (2FA):** Mantenha o 2FA ativado em todos os sistemas e contas, preferindo aplicativos autenticadores em vez de SMS.
6. **Mantenha Dispositivos Atualizados:** Mantenha sistemas operacionais, navegadores e antivírus sempre atualizados para corrigir vulnerabilidades conhecidas.

5. Procedimento de Resposta a Incidentes (Conforme Resolução CMN 4.893/21)

Em cumprimento aos requisitos de registro, controle e mitigação de incidentes cibernéticos da norma (Art. 3º, IV):

Caso Identifique uma Suspeita ou Sofra uma Fraude:

1. **Isolamento Imediato:**
   - Se clicou em um link ou baixou arquivo suspeito no computador/celular corporativo, desconecte o dispositivo da internet (Wi-Fi e cabo).
2. **Notificação da Equipe de Segurança / TI:**
   - Reporte imediatamente ocorrências, e-mails de phishing ou comportamento anômalo ao time de segurança da informação ou canal interno de incidentes.
3. **Bloqueio de Credenciais:**
   - Altere imediatamente as senhas das contas afetadas a partir de um dispositivo seguro.
4. **Comunicação às Instituições Financeiras:**
   - Em caso de perda de valores ou vazamento de dados bancários, acione os canais oficiais de atendimento da instituição para bloqueio de transações e acionamento do **Mecanismo Especial de Devolução (MED)**, quando aplicável.
5. **Registro de Ocorrência:**
   - Preserve evidências (prints, e-mails originais com cabeçalho, extratos) e registre o Boletim de Ocorrência junto às autoridades competentes.