PROGRAMA DE CONSCIENTIZAÇÃO – SEGURANÇA DA INFORMAÇÃO

Sumário

1. INTRODUÇÃO

Tendo em vista a crescente onda de ataques cibernéticos, o aumento da regulamentação em relação à privacidade de dados e a maior sensibilidade do mercado a violações de dados, o IT Cyber Security da Biotrop no uso de suas atribuições implementou um programa de treinamentos de conscientização em "Segurança da Informação" para capacitar todos os colaboradores da organização.

Pontos abordados neste programa:

- Criação de um canal de comunicação com o IT Cyber Security, permitindo que os colaboradores informem e submetam atividades suspeitas;

- Criação e divulgação de conteúdos sobre temas relacionados à segurança da informação;

- Envio de *Phishing* simulado para toda a organização, a fim de avaliar a propensão dos colaboradores a clicarem em links maliciosos;

- Criação de campanha de treinamento, envolvendo o assunto *Phishing*, obrigatória para colaboradores que clicaram em *Phishing* simulado;

- Criação de campanha de treinamento de conscientização em Segurança da Informação abordando vários temas.

O objetivo principal deste programa é diminuir a exposição à ameaças que exploram o fator humano como vetor de ataque.

2. CANAL DE COMUNICAÇÃO

O IT Cyber Security criou o canal de comunicação – cyber@biotrop.com.br - para que os colaboradores possam encaminhar e-mails com conteúdo duvidoso, informarem atividades suspeitas ou comunicarem incidentes de segurança.

Juntamente com a divulgação deste canal, realizada por e-mail para todos os colaboradores, foi disponibilizada uma cartilha sobre o tema *Phishing* (Anexo A) contemplando as características deste tipo de ataque.

Figura 1 - Informativo enviado por e-mail

3. PLATAFORMA DE TREINAMENTOS

Os colaboradores da Biotrop receberão treinamentos e serão capacitados em segurança da informação, através da plataforma de última geração da KnowBe4.

A KnowBe4 é uma organização líder mundial em Treinamentos de Conscientização sobre Segurança, e sua plataforma permite a realização de testes de Phishing simulados, treinamentos evolvendo vários temas ligados à segurança da informação, bem como avaliações para atestar o conhecimento dos usuários.

4. TESTE SIMULADO DE *PHISHING*

4.1. Campanha base

Para determinar a propensão dos colaboradores caírem em um ataque desta natureza, foi realizado o envio de um *Phishing* simulado para toda a organização usando a plataforma da KnowBe4.

Figura 2 - Campanha de Phishing na plataforma KnowBe4

O e-mail enviado informava que o colaborador possuía um novo correio de voz e deveria clicar em um link para reproduzi-lo.

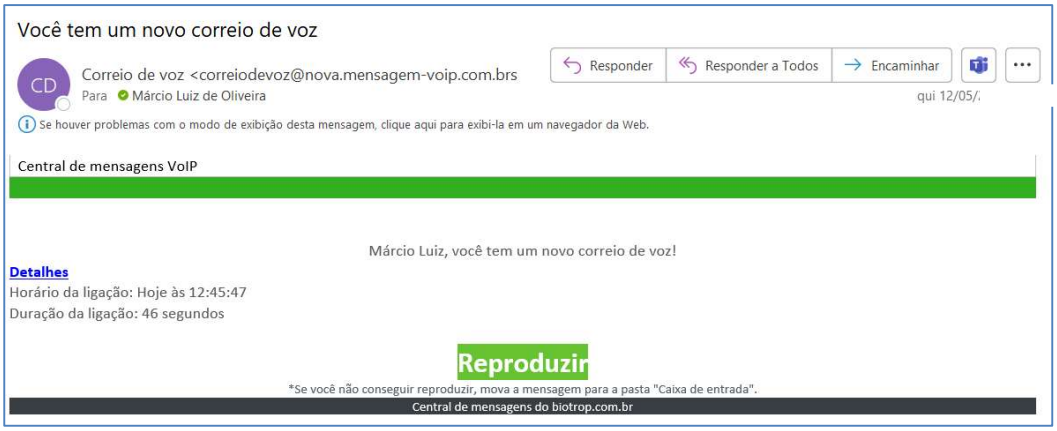

Figura 3 - *Phishing* simulado enviado

4.1.1. Resultado da campanha base

Na campanha base, o *Phishing* simulado foi disparado para 342 destinatários.

105 colaboradores clicaram no link malicioso contido no e-mail, o que corresponde a 30,7% do total de destinatários.

Figura 4 - Resultado campanha base *Phishing*

4.1.2. Comunicação após realização do *Phishing* simulado

Ao término da campanha base de *Phishing* simulado, os colaboradores foram informados sobre o teste de segurança realizado, quais foram os resultados obtidos e os sinais de alerta que poderiam ter sido observados para identificar a mensagem como um possível *Phishing*.

Figura 5 - Comunicado do teste de segurança realizado

Sinais de alerta que poderiam ter sido observados para identificar a mensagem como um possível *Phishing.*

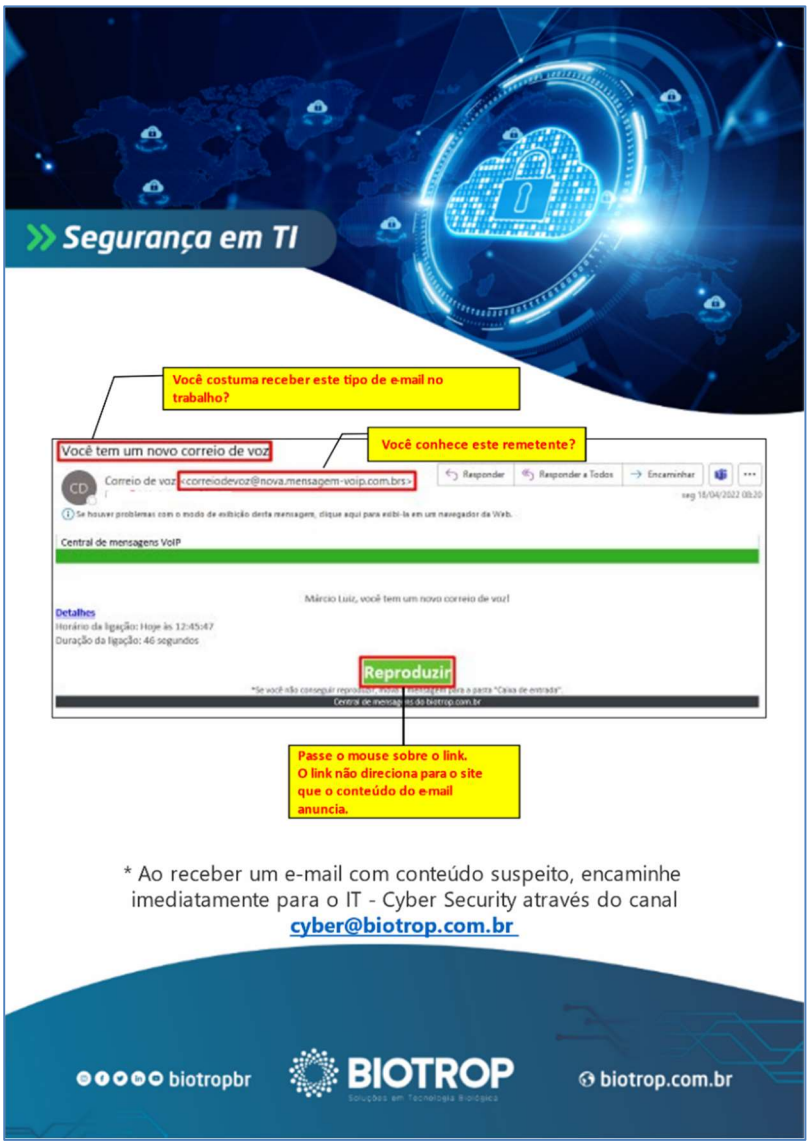

Figura 6 - Sinais de alerta no teste de *Phishing*

Os colaboradores que não abriram e/ou não clicaram no *Phishing* simulado, receberam um e-mail parabenizando sua atitude e reforçando que este tipo de comportamento ajuda a reduzir a exposição da organização à certos tipos de ameaças.

Parabéns!

Recentemente você participou de um teste de Phishing Simulado e não clicou no link malicioso que havia na mensagem.
Este tipo de atitude ajuda a diminuir a exposição da empresa à determinadas ameaças e riscos, contribuindo fortemente para o sigilo e segurança dos dados que utilizamos.

Reforçamos que, ao receber um e-mail com conteúdo suspeito, encaminhe imediatamente para o IT - Cyber Security através do canal cyber@biotrop.com.br

Att,
Cyber Security

BIOTROP Soluções em Tecnologia Biológica

IT - Cyber Security
cyber@biotrop.com.br
+55 (41) 3099-7300
Escritório: Av. Benedito Storani, 1425 - Sala 219
Vinhedo - SP | CEP: 13.289-014
Fábrica: Rua Emilio Romani, 1150
CIC - Curitiba - PR - CEP: 81.460-020

Figura 7 - E-mail enviado para colaboradores que não clicaram no *Phishing* simulado

4.1.3. Treinamento obrigatório – *Phishing*

Os colaboradores que abriram e clicaram no link, presente na mensagem de *Phishing* simulado, terão que participar de um treinamento obrigatório sobre o tema *Phishing*.

Este treinamento contempla:

a) Fundamentos do phishing;
b) Como identificar ataques de phishing.

Figura 8 - Treinamento obrigatório de Phishing na plataforma KnowBe4

4.2. Campanhas recorrentes de *Phishing*

Novas campanhas permitirão avaliar a evolução dos colaboradores.

E-mails de *Phishing* simulado serão enviados através de campanhas automatizadas e de forma recorrente (mensalmente ou quinzenalmente).

5. TREINAMENTOS EM SEGURANÇA DA INFORMAÇÃO

Foi criada uma campanha de treinamento de Conscientização em Segurança, para que todos os colaboradores sejam capacitados neste tema.

A campanha criada treinamento contempla:

a) Avaliação de conhecimento sobre conscientização em segurança;
b) Princípios básicos da conscientização de segurança;
c) Sua função: A segurança na internet e você.

Figura 9 - Treinamento de Conscientização em Segurança na plataforma KnowBe4

6. CONCLUSÃO

O programa de conscientização descrito neste documento, contribuirá fortemente para o aumento da cultura de segurança da informação dos colaboradores, podendo ser aplicado tanto no ambiente corporativo como também em suas rotinas pessoais fora da organização.

ANEXO A

CARTILHA DE CYBER SECURITY – PHISHING

1. **OBJETIVO**

Apresentar para os nossos colaboradores o conceito de *Phising*, como identificar características deste tipo de ataque e como agir diante do recebimento de e-mails suspeitos.

2. **APLICAÇÃO**

Esta política aplica-se a todas as áreas da Biotrop.

3. **RESPONSABILIDADES**

Colaboradores: Atender as regras descritas nesse procedimento;

4. **CRITÉRIOS**

4.1. **Prazos**

A presente cartilha vigerá enquanto o colaborador fizer parte do quadro de colaboradores de uma das companhia do grupo Aqua.

5. **PROCEDIMENTOS**

5.1. ***Phishing***

Phishing, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;

- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;

- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;

- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. Exemplos de situações envolvendo phishing são:

Páginas falsas de comércio eletrônico ou *Internet Banking*: você recebe um *e-mail*, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um *link*. Ao fazer isto, você é direcionado para uma página *Web* falsa, semelhante ao *site* que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

Páginas falsas de redes sociais ou de companhias aéreas: você recebe uma mensagem contendo um *link* para o *site* da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página *Web* falsa onde é solicitado o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas que passarão a ter acesso ao *site* e poderão efetuar ações em seu nome, como enviar mensagens ou emitir passagens aéreas.

Mensagens contendo formulários: você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

Mensagens contendo *links* para códigos maliciosos: você recebe um *e-mail* que tenta induzi-lo a clicar em um *link*, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você abri-lo/executá-lo, será instalado um código malicioso em seu computador.

Solicitação de recadastramento: você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de *e-mail* está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

Exemplos de tópicos e temas de mensagens de *phishing*.

Tópico	**Tema da mensagem**
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem

Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e Notícias Falsass	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama *online*
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados

Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
***Sites* com dicas de segurança**	aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

5.1.2 Prevenção:

- Fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;

- Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há por que recadastrar dados ou atualizar módulos de segurança);

- Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;

- Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;

- Seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;

- Verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing*. Ao posicionar o *mouse* sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;

- Verifique se a página utiliza conexão segura. *Sites* de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;

- Verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro;

- Acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

6. Como reportar em caso de suspeita

Recebeu um e-mail com as cacterísticas descritas anteriormente?

Não execute qualquer ação solicitada no mesmo (clicar em links, baixar anexos, etc.) e encaminhe o e-mail suspeito imediatemente para a área de IT - Cyber Security, através do canal **cyber@biotrop.com.br**, onde analisaremos e iremos orientá-lo como proceder.