FIAP ON

CYBERSECURITY

Conhecendo A ENGENHARIA SOCIAL

OSMANY DANTAS RIBEIRO DE ARRUDA

8

LISTA DE FIGURAS

SUMÁRIO

8 CONHECENDO A ENGENHARIA SOCIAL

Com o uso cada vez mais disseminado dos sistemas computacionais, com diversos produtos e serviços a poucos cliques de distância, o fator humano poderá se tornar um atalho para que indivíduos mal-intencionados consigam acessá-los. De acordo com Mitnick e Simon (2006), uma empresa pode adquirir as melhores tecnologias de segurança disponíveis no mercado, pode ter treinado seu pessoal segundo as melhores práticas e, ainda, ter contratado a melhor segurança patrimonial disponível, mesmo assim, continuará vulnerável.

Em seu testemunho ao Congresso norte-americano, Kevin Mitnick declarou ser o fator humano o elo mais fraco da segurança, afirmando ainda que, com frequência, a segurança é apenas uma ilusão que pode ser ainda pior quando crueldade, inocência ou ignorância são adicionadas ao contexto, citando ainda Albert Einstein ao declarar que “Duas coisas são infinitas: o universo e a estupidez humana. Mas, em relação ao universo, ainda não tenho certeza”.

Greavu-Serban e Serban (2014) afirmam que a engenharia social ainda é um tabu, envolvendo o uso de habilidades sociais para obtenção dos mais variados tipos de informações, como nomes de usuários e senhas utilizados em sistemas de autenticação e dados de cartões de crédito, dentre muitas outras possibilidades.

O US-CERT afirma que nesse tipo de ataque, o atacante se vale de suas habilidades sociais para obter ou comprometer informações sob responsabilidade da empresa ou mesmo seus sistemas computacionais. Os atacantes, geralmente conhecidos como engenheiros sociais, são pessoas bem articuladas, muito seguras de si e amáveis ao extremo, que dessa forma conseguem atrair a atenção e conquistar a confiança daqueles com os quais se relaciona, por meio de diversas técnicas diferentes, extraindo ou acessando as informações que desejam.

Independentemente da forma como possa vir a ocorrer, é amplamente sabido que o vazamento de informações pode ter graves reflexos sobre sob vários aspectos de uma empresa, dos quais destacam-se aqui as perdas financeiras decorrentes de indenizações e os danos à imagem corporativa da empresa, os quais podem resultar na perda de receitas e dificuldade em fechar novos negócios.

Logo, sendo a engenharia social uma modalidade de ataque altamente eficiente, e essencialmente não tecnológico, é imprescindível que as empresas adotem políticas e procedimentos especializados para mitigar os riscos por ela originados.

Todo o exposto foi claramente sintetizado por Bruce Schneier (2000) em uma única frase, ao afirmar que: “Segurança é um processo, não um produto”.

De acordo com Schneier (2000), os produtos podem oferecer alguma proteção, todavia, a única maneira de efetivamente fazer negócios em um mundo inseguro, vem da implementação de processos que reconheçam a insegurança inerente aos produtos. Logo, a melhor opção é **mitigar o risco de exposição independentemente de produtos e *patches***.

Em pesquisa realizada em 2016, a Balabit, empresa provedora de soluções em gerenciamento de acesso privilegiado (Privileged Access Management - PAM), apurou que mais de 80% dos entrevistados consideram a engenharia social como o principal método de hacking:

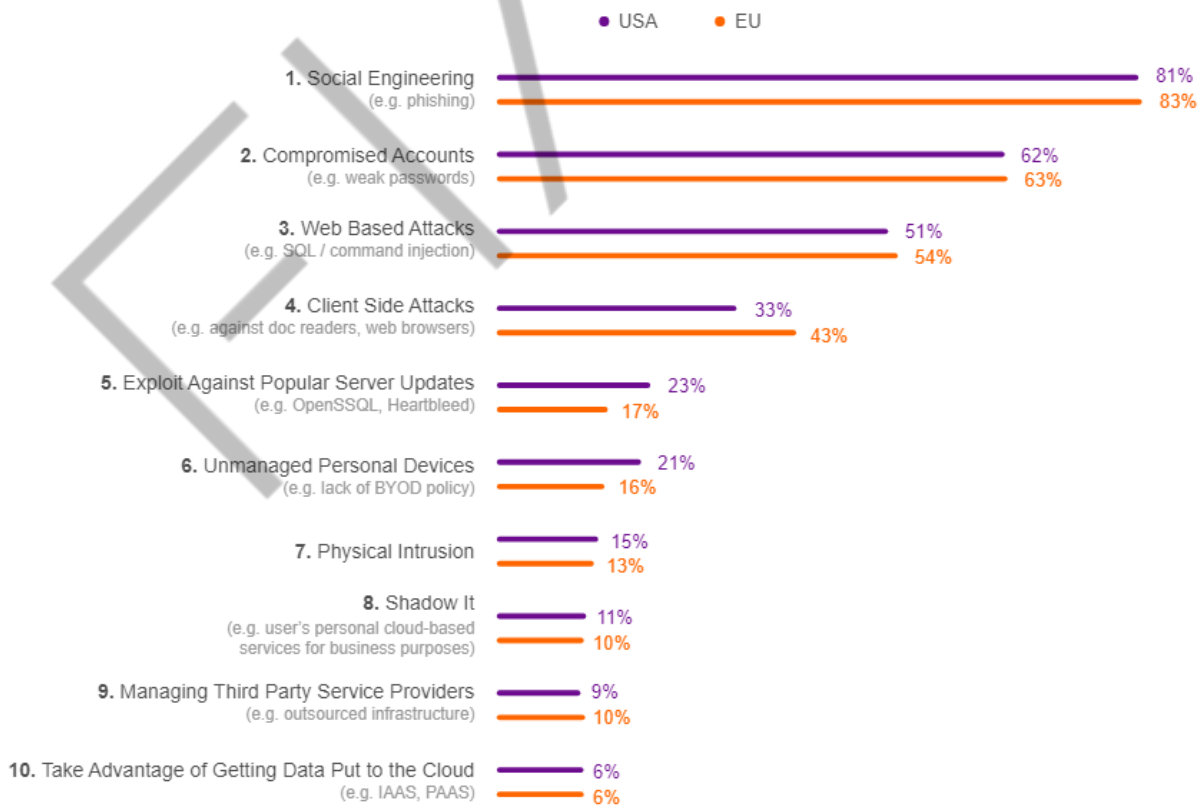

Figura 8.1 – Top 10 Most Popular Hacking Methods
Fonte: Balabit (2016)

Essa pesquisa mostrou ainda que 40% dos entrevistados estavam cientes de que ferramentas normalmente utilizadas como primeira linha de defesa, a exemplo dos *firewalls*, não são eficazes na prevenção de ataques cibernéticos, confirmando dessa maneira, o anteriormente já afirmado por Bruce Schneier.

8.1 O perfil de um engenheiro social

Segundo Mitnick e Simon (2006), o perfil de um engenheiro social é produto da combinação entre uma inclinação para enganar as pessoas e dos talentos da influência e persuasão. Em seu depoimento no Congresso norte-americano, aos senadores Lieberman e Thompson, Mitnick testemunhou ter conseguido acesso não autorizado a sistemas computacionais corporativos altamente protegidos valendo-se de meios técnicos e não técnicos para obter o código-fonte de diversos sistemas operacionais e dispositivos de telecomunicações, a fim de estudar seu funcionamento interno e, assim, descobrir suas vulnerabilidades.

Segundo Ministério Público do Estado de São Paulo – MPSP (2017), o engenheiro social é um indivíduo perspicaz e habilidoso que se aproveita de descuidos e até da ingenuidade de sua vítima, como excesso de exposição em redes sociais ou divulgação de senhas pessoais a terceiros, para obtenção de informações sigilosas.

Também no ambiente corporativo, a engenharia é amplamente empregada tendo o engenheiro social interesse por qualquer fonte de informação que possa vir a lhe ser útil, como documentos esquecidos em impressoras ou copiadoras.

Atas e relatórios sobre as mesas, ao final de reuniões, são fontes de informações especialmente ricas, na medida em que podem conter assinaturas, números de telefones, e-mails, endereços, agendas, demonstrativos financeiros.

Crachás expostos fora do ambiente da empresa e catracas sem o devido controle de acesso também podem vir a comprometer o sistema de segurança de qualquer empresa, cabendo aqui, mais uma vez ressaltar que o acesso a nenhuma das referidas fontes de informação necessita de meios tecnológicos.

Geralmente, os engenheiros sociais preferem abordagens indiretas, por exemplo, por meio da Internet ou de telefonemas preparando-se, entretanto, de maneira ainda mais meticulosa que quando de um ataque direto.

Ainda segundo o MPSP (2017), em ataques diretos (presencialmente) os engenheiros sociais se aproveitam do descuido e da ingenuidade dos clientes, por exemplo, em agências bancárias, para realizar troca de cartões em terminais de autoatendimento ou, ainda, para obter informações relacionadas a contas e senhas, agindo como pessoas bem-intencionadas e interessadas em ajudar o próximo. A verbalização de informações a terceiros em outro ambiente qualquer também pode representar fator de risco, na medida em os engenheiros sociais utilizam dados pessoais divulgados em locais públicos, como restaurantes, aeroportos, elevadores, táxis e hotéis, dentre outros. Os engenheiros sociais atingem suas vítimas explorando principalmente os seguintes sentimentos humanos (MPSP, 2017):

- Curiosidade: abordam assuntos populares ou atrativos para induzir o clique em arquivos maliciosos ou links que direcionam a sites falsos.
- Preguiça: tiram proveito da negligência de alguns funcionários em seguir regras corporativas.
- Solidariedade: criam falsas campanhas de doações, oferecem descontos e promoções; são extremamente prestativos em ajudar em transações nos terminais bancários de autoatendimento.
- Vaidade: ofertam falsos produtos e serviços em condições imperdíveis, com o intuito de estimular a futilidade e o poder.
- Medo: usam a persuasão e o convencimento para obter informações.
- Ganância: oferecem falsas oportunidades de ganhos altos em pouco tempo.
- Confiança: utilizam o nome de grandes corporações e de entidades governamentais para obter informações.
- Ingenuidade: exploram o desconhecimento técnico e informacional das vítimas.

Para obter sucesso em seu ataque, o engenheiro social deve conhecer bem o jargão corporativo e a estrutura da empresa alvo, por exemplo, conhecendo nomes

de funcionários, suas funções e cargos. Deverá também prever e se precaver contra situações adversas como, se durante um contato telefônico, o atendente pedir o ramal para um retorno posterior, pois no momento, o sistema está indisponível. O engenheiro deverá responder algo como “meu ramal é 4321, mas estarei fora o resto da tarde em reunião com minha gerência. Posso voltar a ligar quando estiver disponível?”.

Geralmente, são muito atenciosos, educados e fazem o possível para agradar e conquistar a simpatia e confiança do alvo, entretanto, não hesitam quando condutas menos elegantes se fazem necessárias, como revistar o lixo da empresa em busca de informações.

8.2 Principais técnicas de engenharia social

Os engenheiros sociais se utilizam das mais variadas técnicas para implementação de seus ataques, algumas das quais são destacadas nesta sessão.

8.2.1 Phishing

De acordo com o CERT.Br (2012), *phishing* é o tipo de fraude na qual um golpista tenta obter dados pessoais e financeiros de um usuário, por meio do uso combinado de meios técnicos e engenharia social.

O *phishing* é praticado com o envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de alguma instituição conhecida como, um banco, uma empresa ou um site popular;
- procuram atrair a atenção do usuário aguçando sua curiosidade, apelando à sua caridade ou, ainda, oferecendo possibilidade de vantagens financeiras dentre outras possibilidades;
- advertem que o não atendimento aos procedimentos solicitados poderá ter sérias implicações como a inscrição em serviços de proteção ao crédito ou o cancelamento de um cartão de crédito;
- Induzem o usuário a fornecer dados pessoais e/ou financeiros por meio de páginas web falsas que imitam as páginas oficiais de alguma instituição; que

tentam instalar códigos maliciosos destinados à coleta de informações ou, ainda, pelo preenchimento de formulários contidos na mensagem ou em páginas web.

A mitigação desse tipo de ataque exige atenção e ações, geralmente simples, por parte do usuário tais como: verificar as URLs apresentadas em *links* contidos na mensagem, uma vez que elas costumam ser ofuscadas pelo atacante (*URL Obfuscation*); não fazer recadastramento nem atualização de módulos de segurança bancária com base em mensagens, mesmo que aparentem ser legítimas; não confiar no conteúdo de uma mensagem somente porque o remetente é conhecido e verificar o uso de HTTPS, dentre outras medidas.

De acordo com relatório da Global Information Security, no ano de 2019 a fraude phishing esteve em primeiro lugar entre as 10 maiores ameaças cibernéticas relacionadas às organizações.

Figura 8.2 – As 10 maiores ameaças cibernéticas
Fonte: Global Information Security Survey (2019)

8.2.2 “Furto” de identidade (*Identity theft*)

O Cert.BR (2012) define “furto” de identidade como a tentativa de um atacante de se passar por outra pessoa, dessa maneira, assumindo uma identidade falsa, geralmente com objetivo de obter alguma vantagem indevida, podendo ser considerado como um tipo de crime contra a fé pública, tipificado como falsa identidade. Como exemplos de tal prática no mundo real, pode-se citar a abertura de uma empresa ou de uma conta bancária por um terceiro, usando os dados da vítima.

Já na Internet, pode-se tomar como exemplos alguém que crie um perfil em uma rede social ou envie e-mails com os dados de um terceiro. É comum encontrar-se também o termo “roubo” de identidade, entretanto, há que se observar que o emprego de ambos os termos (furto ou roubo) é meramente ilustrativo, uma vez que não correspondem à tipificação jurídica atribuída a cada um deles.

A prevenção contra esse tipo de ataque também passa por várias medidas por parte do usuário, das quais cita-se como exemplos: evitar a divulgação de dados pessoais (nome completo, endereço, RG, CPF e semelhantes) e de autenticação em serviços (*usernames* e senhas, números de contas bancárias e de cartões de crédito, dentre outros); utilizar senhas fortes e periodicamente substituídas e não preencher cadastros em *sites* desconhecidos ou não confiáveis.

8.2.3 Personificação (*Impersonation*)

A personificação é uma técnica utilizada pelo engenheiro social para obter acesso a um sistema ou rede, geralmente, com intenção de cometer fraudes, espionagem industrial ou “roubo” de identidade. Essa técnica difere de outras empregadas pela engenharia social na medida em que é executada pessoalmente, e não por telefone ou por e-mail.

O engenheiro social tenta personificar ou desempenhar papel semelhante ao de alguém, se ele confia ou obedece, induzindo o alvo a permitir acesso aos locais, sistemas ou informações desejadas por ele. Essa técnica explora a tendência natural de se dar crédito às pessoas e de se respeitar a autoridade/ hierarquia, manipulando deliberadamente o alvo a fim de obter as informações desejadas sem que ele, nem sequer, perceba uma violação de segurança.

Alguns dos papéis mais frequentemente fraudados pelo atacante são o de entregador, leiturista (especialmente água ou energia elétrica), gerente ou diretor, alguém do suporte de TI ou, até mesmo, um terceiro de confiança (como um consultor ou auditor externo), dentre outros.

Eventualmente, o combate a essa técnica poderá causar algum constrangimento ao alvo, no sentido de que a verificação das credenciais e do nível de acesso de um superior hierárquico ou terceiro de confiança, por exemplo, antes de atender às suas solicitações ou questionamentos, geralmente não é a atitude esperada por eles.

8.2.4 Baiting

Nesta técnica, o atacante, de alguma forma, disponibiliza um dispositivo infectado com um *malware* para um alvo, o qual nem sempre é específico. Por exemplo, deixa um *pendrive* ou um CD com etiqueta indicando Folha de Pagamento, dentro de um elevador do prédio da empresa. Sua intenção é aguçar a curiosidade dos potenciais alvos, para que então interajam com o dispositivo, e dessa forma, se tiverem privilégios suficientes, inadvertidamente instalarem o código malicioso.

8.2.5 Pretexting

Pretexting pode ser definido como a prática de se apresentar como outra pessoa para obter informações privadas. Mais do que apenas criar uma mentira, em alguns casos, uma identidade totalmente nova poderá ser criada para, em seguida, ser usada para manipular o recebimento de informações.

O *pretexting* também pode ser usado para se passar por pessoas em certas posições ou funções que nunca exerceram, exigindo que o engenheiro social desenvolva diversos pretextos diferentes ao longo de sua carreira, tendo todos eles a pesquisa como denominador comum.

Uma forma fácil e eficiente de implementação dessa técnica pode tomar como base a coleta de informações gerais a respeito do alvo na Internet, por exemplo, por meio de redes sociais, as quais geralmente oferecem os subsídios necessários a um primeiro contato do engenheiro social com o alvo.

8.2.6 Quid pro quo

Traduzida do latim, essa expressão significa “isto por aquilo”, a qual no contexto da engenharia social pode ser entendida como dar um pouco ao alvo, para ganhar muito. Ou seja, o engenheiro social oferece algumas informações, às quais sabe que o alvo responderá bem, por exemplo: “A secretária do diretor é muito bonita! Qual o nome dela, mesmo?”.

Outra abordagem bastante difundida recai sobre falsas pesquisas, nas quais alvos, específicos ou não, respondem a questionários em troca de brindes. Pode parecer difícil de acreditar, mas houve (?!) época em que funcionários de empresas chegavam a trocar suas senhas por canetas baratas ou mesmo barras de chocolates!!

8.2.7 *Gift giving* (presentear)

Todos gostam de ser presenteados, e isso desencadeia o princípio de influência chamado reciprocidade, segundo o qual, ao ser presenteada, a pessoa sente-se compelida a retribuir. Mas como se pode presentear alguém que se acabou de encontrar? Nesse caso, o mais adequado seria a validação. Valide seus pensamentos e ideias usando a escuta ativa e fazendo perguntas. Dê um pouco de informação sobre você (*quid pro quo*) e você receberá o presente de sua informação.

Outra maneira de presentear, consiste em levar algo com você como um antisséptico para as mãos ou chiclete. Isso funciona especialmente bem em situações de viagem, como em um avião ou trem. O ponto alto da oferta de presentes é que não importa se a pessoa quer o presente, se gosta de você ou mesmo o valor monetário dele. A oferta em si criará o sentimento, e o sentimento garantirá que o presente seja devolvido.

8.2.8 Spear phishing

São ataques persistentes e sofisticados contra organizações governamentais e empresas de todos os tamanhos. Assim como o *phishing*, o *spear phishing* também se vale de mensagens de *e-mail*, porém, dessa vez, aparentemente originadas por fonte confiável, por exemplo, um parceiro de negócio.

De acordo com o *Global Threat Intelligence Report* (2016), o *spear phishing* cresceu de 2% em 2014 para 17% em 2015 nas categorias de incidentes de segurança identificados do ano.

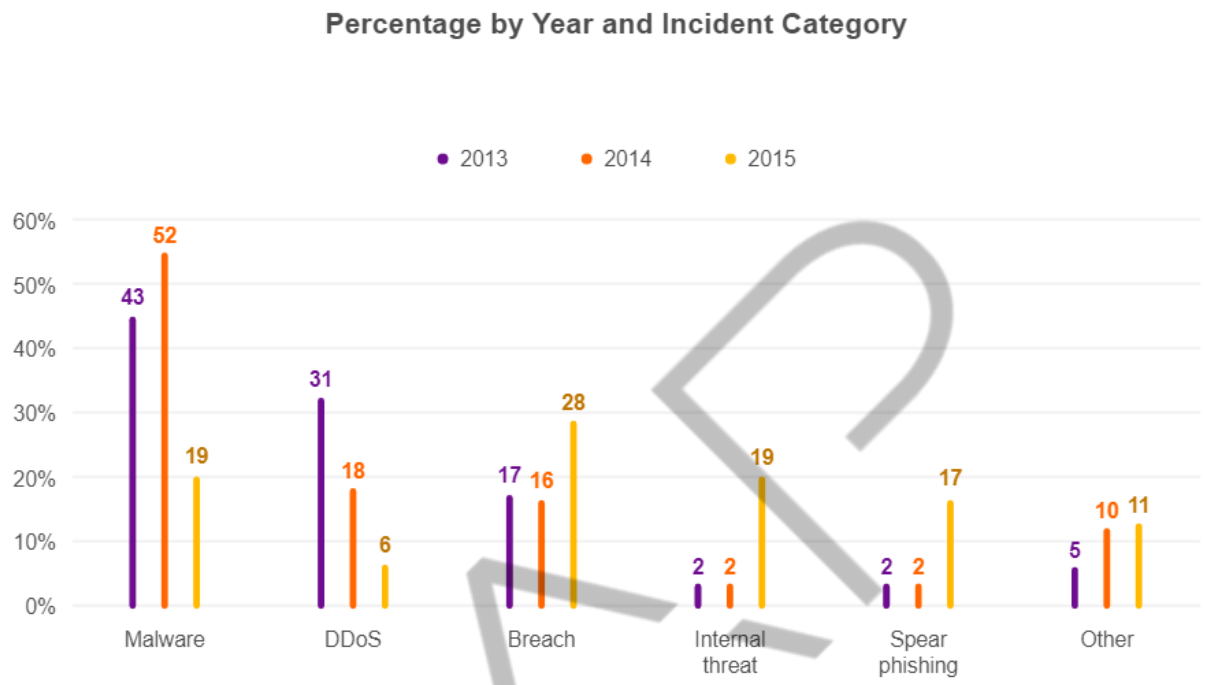

Figura 8.3 – Global Threat Intelligence Report
Fonte: Dimension Data (2016)

Ainda de acordo com o relatório, geralmente, esse tipo de ataque é direcionado a usuários específicos das organizações, com objetivo de obter *usernames*, senhas e números de cartões de crédito, dentre outras informações.

8.2.9 Tailgating

Também conhecido como *piggybacking*, neste ataque alguém sem credenciais adequadas segue uma pessoa autorizada ao adentrar uma área restrita (Figura *Tailgating*). Uma abordagem comum do *tailgating* ocorre quando um falso entregador espera até que um funcionário autorizado abra uma porta em alguma área da empresa, quando então, carregando uma grande caixa, solicita ao funcionário que segure a porta para que ele possa passar.

Normalmente, esse tipo de ataque só funciona em pequenas e médias corporações, uma vez que nas maiores, em regra, os funcionários são obrigados a manter os respectivos cartões de identificação sempre à vista.

Figura 8.4 – *Tailgating*
Fonte: Banco de imagens Shutterstock (2020)

8.2.10 Shoulder surfing

Certamente, esta é uma das abordagens da engenharia social mais simples e corriqueira, algumas vezes, praticada inocentemente pela maioria das pessoas, não apenas por engenheiros sociais. Resume-se àquela olhadinha por cima do ombro quando alguém preenche um formulário ou digita a respectiva senha no computador, num caixa eletrônico ou numa máquina de cartões de débito/crédito, dentre muitas outras possibilidades.

Figura 8.5 – Shoulder surfing
Fonte: Banco de imagens Shutterstock (2020)

8.2.11 Dumpster diving

Também uma abordagem não técnica amplamente utilizada por engenheiros sociais, consistindo na inspeção do conteúdo do lixo do alvo: uma empresa ou indivíduo, em busca de informações úteis como faturas de cartões de crédito, extratos bancários, cartão comercial do instalador do sistema de alarme, atas de reuniões e memorandos dentre outros documentos incorretamente descartados ou mal fragmentados.

Figura 8.6 – *Dumpster diving*
Fonte: Banco de imagens Shutterstock (2020)

8.2.12 URL Obfuscation

A URL Obfuscation é uma técnica na qual um endereço *web* malicioso é obscurecido ou oculto de forma a imitar a URL original de um *website* legítimo, com objetivo de enviar o usuário a um *website* falso em vez do solicitado.

Os *websites* falsificados, geralmente, são bastante semelhantes aos originais, facilmente enganando usuários desatentos, os quais acabam por fornecer suas credenciais de acesso (*login*) no site original.

Há várias formas de se ofuscar uma URL. Uma das mais simples é a dos “encurtadores” (URL *shortener*), como o *bitly*, bastando fornecer a ele a URL desejada, clicar no botão *shorten*, e a URL será encurtada. Isso pode ajudar bastante na divulgação e digitação de URLs longas, entretanto, pode também ser utilizado para disfarçar e dificultar a identificação de uma URL maliciosa.

Como exemplo, pode-se acessar a página inicial do bilty, em https://bitly.com/, e fornecer a URL www.fiap.com.br. Após encurtada, ela ficará como https://bit.ly/2Y6HOdL, conforme figura abaixo.

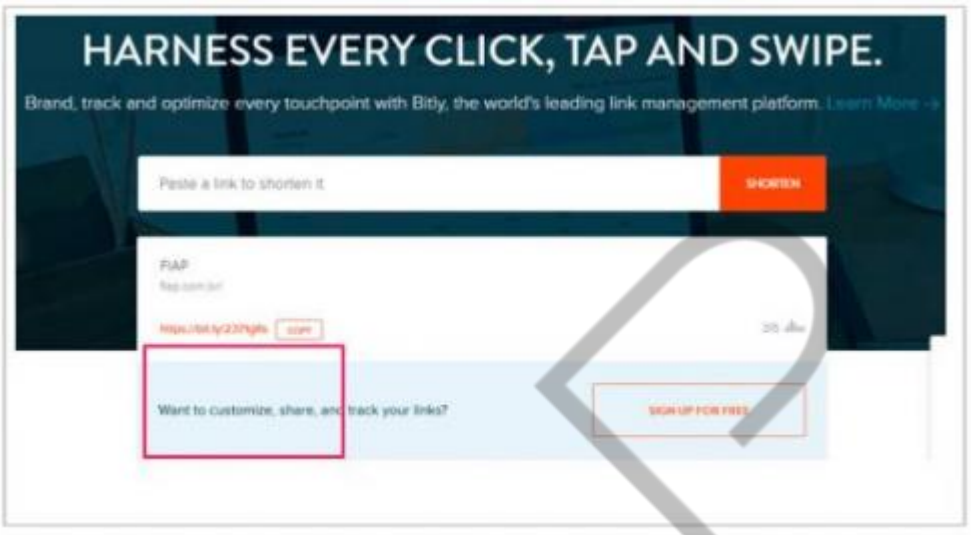

Figura 8.7 – *URL Obfuscation*
Fonte: Bilty.com (2020)

Pelo destaque na figura acima, pode-se observar a URL original (fiap.com.br) e a URL ofuscada (https://bit.ly/2Y6HOdL). Vale lembrar que esses endereços têm tempo de vida muito curto, e que, provavelmente, nesse instante ele não esteja mais disponível, Outra forma de ofuscar uma URL é fazendo issomanualmente, com base no endereço IP do alvo. Tomemos como exemplo um dos endereços IP do GOOGLE: 216.58.202.100. Convertendo cada octeto para seu equivalente em hexadecimal tem-se:

- 216: 0xD8
- 58: 0x3A
- 202: 0xCA
- 100: 0x64

Ao juntar-se os valores calculados, obtém-se 0xD83ACA64, do qual, ao ser convertido para a base decimal, retorna o valor 3627731556. Ao reescrever-se a URL original com esse valor, tem-se http://3627731556, que ao ser fornecida ao navegador, levará o usuário ao website do GOOGLE.

Outro método utilizado para ofuscação da URL é eliminado o “http://” de sua estruturação. Caracteres não alfanuméricos como @, : ,? e %, dentre outros, não

podem fazer parte de URLs, uma vez que possuem significado especial fazendo, portanto, com que o navegador tente interpretá-los.

Logo, quando precisar enviar esses caracteres como parâmetros via solicitação GET, eles precisarão ser codificados na URL. Portanto, o caractere “?” deverá ser transformado em %3f, o @ em %40 e assim por diante, representando os valores hexadecimais dos caracteres desejados, conforme figura abaixo. Cole esta URL em seu navegador, e veja o resultado:
http://%67%6f%6f%67%6c%65%2e%63%6f%6d .

Tabela ASCII

Dec	Hex	Name	Char	Ctrl+char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Dataline escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Figura 8.8 – Tabela ASCII
Fonte: Google Imagens (2018)

8.3 Pessoas, processos e tecnologias

Do exposto, sabe-se não ser possível garantir a segurança da informação unicamente com base em tecnologias (SCHNEIER, 2000; MITNICK & SIMON, 2006), cabendo mais uma vez salientar ser o fator humano o elo mais fraco da segurança (MITNICK & SIMON, 2006).

Schneier (2000) enfatiza ainda ser a segurança um processo, que permite concluir, em função de tudo isso, que a segurança da informação se encontra diretamente relacionada a três fatores: pessoas, processos e tecnologias. Assim sendo, mais do que apenas a devida conscientização das pessoas em relação aos riscos da engenharia social, elas deverão também ser adequadamente treinadas a fim de identificarem e protegerem-se de tais ataques, observando-se que, como as ameaças são dinâmicas e encontram-se em constante evolução, também a conscientização e o treinamento deverão ser periodicamente reciclados.

As diversas tecnologias disponíveis para proteção da informação, como IPSs, proxies e filtros de conteúdo, dentre outras, devem ser combinadas de forma a caracterizarem uma solução, e não apenas um conjunto de diferentes dispositivos cuidando isoladamente de pontos específicos relacionados à segurança da informação. Isso poderá ser conseguido mediante a adequada aplicação das normas técnicas, destacando-se, dentre outras, as NBRs ISO 27001 e ISO 27002, as quais oferecem fundamental contribuição para a construção dos processos que suportarão a segurança da informação (SI), inclusive produzindo políticas de segurança sólidas e com real alinhamento entre a SI e os objetivos/necessidades de negócio.

Em termos práticos, o conhecimento sobre as técnicas de engenharia social pode contribuir consideravelmente para atualização e reforço das políticas de segurança, um dos instrumentos mais importantes para suporte à segurança da informação no ambiente corporativo.

Tome-se como exemplo o *shoulder surfing*, uma abordagem não técnica, típica do comportamento humano, mas que sabidamente pode levar ao vazamento de informações relevantes. Entretanto, em termos práticos, fica bastante difícil proibir que as pessoas passem por detrás umas das outras, logo, algumas contramedidas básicas surgem: (a) do uso de filtros de privacidade para monitores (Figura Filtro de privacidade para monitores), os quais impedem a visão lateral em ângulos maiores que 45º ou 60º (em média); (b) da entrada da proteção de tela após determinado período de ociosidade; e (c) do bloqueio automático do console após determinado certo tempo de atividade da proteção de tela.

O *tailgating* também poderá ser consideravelmente mitigado se as políticas de segurança exigirem o uso de crachás nas dependências da empresa, e o treinamento

dos usuários para instruí-los a notificar seus superiores ou pessoal da segurança física sobre a presença de indivíduos não identificados em setores restritos da empresa.

As políticas de segurança podem contribuir para mitigação do *dumpster diving* ao determinar que o descarte de papéis, em sentido amplo, deve ser iniciado com sua devida fragmentação, incluindo-se desde um simples *post-it* fixado à estação de trabalho, no qual pode ser encontrado o contato de algum fornecedor ou colaborador, até a cópia de uma ata de reunião deixada sobre alguma mesa.

Enfim, do exposto depreende-se que o conhecimento sobre as técnicas de engenharia social pode efetivamente tornar as políticas de segurança mais eficientes e aderentes ao ambiente corporativo, porém, desde que seja efetivamente divulgada, e que suas determinações sejam adequadamente assimiladas e praticadas pelos colaboradores da empresa.

Figura 8.9 – Filtro de privacidade para monitores
Fonte: 2013.phdays.com (2018)

8.4 Evitando a engenharia social

Poderá ser bastante difícil frustrar ataques por engenharia social se os indivíduos, em ambiente corporativo ou não, não reconhecerem esse tipo de ataque

ou não tiverem consciência de suas consequências. Isso poderá levar o indivíduo a ignorar cuidados básicos, deixando-se envolver pela educação e simpatia do engenheiro social e, assim, sem perceber com quem realmente se está lidando, nem quais são as suas reais intenções, comece a fornecer informações como forma de retribuição à atenção e gentilezas recebidas.

Em ambientes corporativos, as políticas de segurança constituem importante instrumento para prevenção das ações dos engenheiros sociais, ajudando a preparar os colaboradores para reconhecer e repelir esse tipo de ataque.

Dentre outras recomendações, o US-Cert (2017) coloca ainda:

- Suspeite de telefonemas não solicitados, visitas ou mensagens de *e-mail* indagando por funcionários ou solicitando outras informações internas. Se um indivíduo desconhecido alegar pertencer a uma organização legítima, tente verificar sua identidade diretamente com a empresa.
- Não forneça informações pessoais nem da organização - incluindo a infra-estrutura ou redes dessa última, a menos que tenha certeza da autoridade do solicitante.
- Não envie informações confidenciais pela *Internet* antes de verificar a segurança de um *site*.
- Verifique a URL dos *sites*. *Sites* maliciosos podem parecer idênticos a um *site* legítimo, mas a URL pode usar uma variação na ortografia ou em um domínio diferente (por exemplo, .*com* vs. .*net*).
- Se não tiver certeza se uma solicitação via *e-mail* é legítima, tente confirmá-la entrando em contato diretamente com a empresa. Não use informações de contato fornecidas em um *site* relacionado à solicitação. Em vez disso, verifique prévias validações das informações de contato. Informações sobre ataques de *phishing* conhecidos também estão disponíveis *on-line* em grupos como o Anti-Phishing Working Group (http://www.antiphishing.org).
- Instale e mantenha *software* antivírus, *firewalls* e filtros de *e-mail* para reduzir parte desse tráfego.

- Aproveite os recursos *antiphishing* oferecidos por seu cliente de *e-mail* e por seu navegador *web*.

Em seu *white paper* intitulado *Cybersecurity for Everyone, Not Just the IT Department*, a *CompTIA* expressa graficamente a relação entre erros humanos e erros tecnológicos, por meio dos quais é possível observar ser o fator humano o elo mais fraco da segurança.

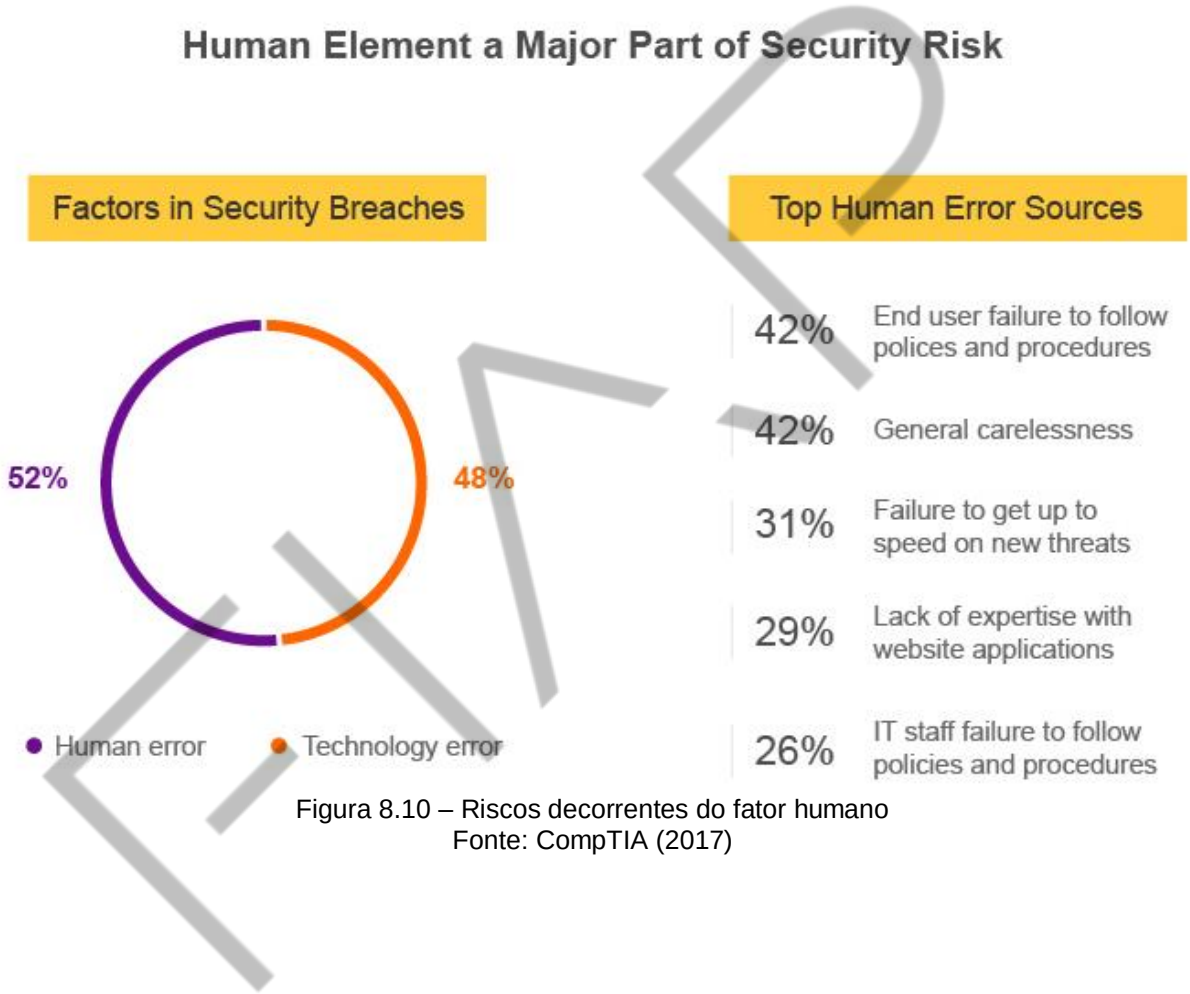

Figura 8.10 – Riscos decorrentes do fator humano
Fonte: CompTIA (2017)

REFERÊNCIAS

5 Social Engineering Attacks to Watch Out For. [s.d.]. Disponível em: <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>. Acesso em: 22 abr. 2020.

BALABIT. **Know Your enemy from the TOP 10 Most Popular Hacking Methods.** [s.d.]. Disponível em: <https://pages.balabit.com/rs/855-UZV-853/images/Balabit-top-10-hacks.pdf>. Acesso em: 22 abr. 2020.

CERT.BR. **Cartilha de Segurança para Inernet.** v.4. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 22 abr. 2020.

COMPTIA. **Cybersecurity For Everyone, Not Just the IT Department.** Disponível em: <https://www.ncsl.org/documents/taskforces/CompTIA_CyberSecure_Human_Error_Whitepaper.pdf>. Acesso em: 22 abr. 2020.

GREAVU-ŞERBAN, V.; ŞERBAN; A.I. **Social Engineering a General Approach.** Informatica Economica. vol.2, n.2, 2014. Disponível em: <http://revistaie.ase.ro/content/70/01%20-%20Greavu,%20Serban.pdf>. Acesso em: 23 abr. 2020.

MITNICK, K. D.; SIMON W. L. **A arte de enganar.** 4. reimpr. São Paulo: Pearson Edfucation, 2006.

MPSP. **ENGENHARIA SOCIAL Saiba como identificar possíveis armadilhas e se proteger de golpes.** 1. ed. 2017. Disponível em: <http://www.mpsp.mp.br/portal/pls/portal/!PORTAL.wwpob_page.show?_docname=2621804.PDF>. Acesso em: 23 abr. 2020.

MYSECURITYAWARENESS. **What is Impersonation in Social Engineering?**. 2018. Disponível em: <http://www.mysecurityawareness.com/article.php?article=384&title=what-is-impersonation-in-social-engineering#.WukDt4jwaM8>. Acesso em: 23 abr. 2020.

SCHNEIER B. **The process of security.** 2000. Disponível em: <https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html>. Acesso em: 23 abr. 2020.

SOCIAL-ENGINEERING. **Pretexting.** Disponível em: <https://www.social-engineer.org/framework/influencing-others/pretexting/>. Acesso em: 23 abr. 2020.

SOCIAL-ENGINEERING. **Talk to strangers – Part 2: KEEPING THEM ON THE HOOK.** [s.d.]. Disponível em: <https://www.social-engineer.org/newsletter/Social-Engineer.Org%20Newsletter%20Vol.%2004%20Iss.%2042.htm>.2013. Newletter. v4. Issue42. Acesso em: 23 abr. 2020.

US-CERT. **Avoind Social Engineering and Phishing Attacks.** rev. 24 Jan. 2017. Disponível em: <https://www.us-cert.gov/ncas/tips/ST04-014>. Acesso em: 30 abr. 2018.