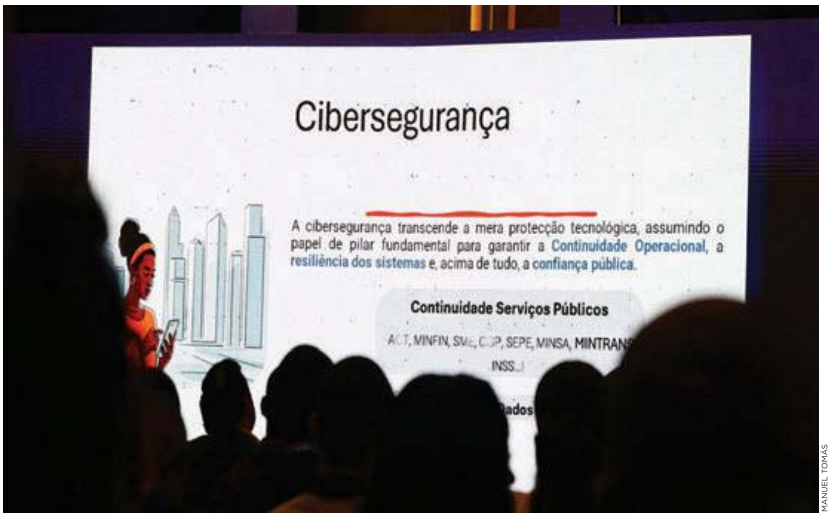
CAPITAL HUMANO

Cibersegurança | quando a burla chega à luz do dia

Num computador, um *firewall* é uma barreira que filtra tráfego malicioso. No nosso quotidiano, o *firewall* humano é a nossa capacidade de discernimento, atenção e auto-controlo perante pedidos suspeitos. É dizer 'não', é parar para validar, confirmar por outro canal. A melhor tecnologia falha sem esta barreira comportamental.

ARIANA ORTET VIGELANDZOON

Coach, Terapeuta Holística e Assessora rganizacional



MANUEL TOMAS

Vivemos numa era em que os maiores assaltos já não acontecem nas ruas, mas nos ecrãs. As novas burlas, cada vez mais sofisticadas, exploram uma vulnerabilidade essencial: a confiança humana. Em Angola e em vários países africanos, têm aumentado os casos de transferências bancárias fraudulentas realizadas dentro das próprias instituições, clonagem de números de telefone e mensagens enviadas por burladores que se fazem passar por companhias de comunicação, de água e de luz, ou até por familiares e amigos. Todos os dias, cidadãos inocentes são apanhados em esquemas que combinam tecnologia com manipulação emocional.

O que é, afinal, a cibersegurança (cybersecurity)? É o conjunto de práticas, políticas e tecnologias que protege redes, sistemas e dados contra acessos não autorizados. Mas, no mundo real, significa também proteger pessoas: as suas identidades, os seus dispositivos e as suas transacções. Segundo a Interpol (Relatório Global de Cibercrime, 2025), mais de 70% dos casos de fraude digital em África nascem de engenharia social — engano psicológico — e não de falhas técnicas. Em Angola, multiplicam-se episódios em que o cliente, acreditando falar com alguém legítimo, autoriza uma transferência para outra conta no mesmo banco. Este golpe é conhecido como *funds transfer fraud* (fraude por transferência de fundos) e já representa, de acordo com a Coalition Inc. (2024), mais de um terço das perdas financeiras associadas a ataques digitais.

A nova face do crime digital é silenciosa e relacional. Os burladores já não precisam de invadir servidores: invadem a confiança humana. Um dos esquemas mais perigosos é a clonagem de contas e mensagens no WhatsApp, muitas vezes suportada por SIM swapping (troca/clonagem do cartão SIM). O burlador duplica o número da vítima, toma controlo da conta e, com a fotografia e o histórico de conversas, dirige-se a familiares e amigos a pedir 'apoio urgente', 'transferência temporária' ou 'ajuda para desbloquear uma conta'. O apelo é emocional e convincente. De acordo com a Kaspersky (Relatório de Segurança Móvel, 2025), a clonagem de WhatsApp está entre as três maiores ameaças digitais no continente, ao lado do *phishing* (captura de credenciais por *sites* falsos) e do *vishing* (chamadas telefónicas fraudulentas).

Também se tornou comum o *spoofing* (falsificação) de números e identidades: chamadas e SMS parecem vir de entidades confiáveis — um banco, a operadora, a empresa de electricidade — e criam um cenário de urgência: 'a sua conta será bloqueada', 'o contrato será cancelado', 'tem um débito imediato'. A pressão do tempo desarma o senso crítico. É nesta brecha que o golpe acontece.

Como nos protegemos? A cibersegurança começa na consciência. Eis um protocolo simples para cidadãos e empresas:

1) Desconfie da urgência
Nenhuma entidade séria exige transferências por WhatsApp ou SMS. Valide pela linha oficial.

2) Nunca partilhe códigos OTP (*one-time password*)
Palavra-passe de uso único) nem PINs. Quem pede códigos, quer entrar na sua conta.

3) Active a verificação em duas etapas (*two-factor authentication*)
Mesmo que o número seja clonado, o intruso esbarra num segundo factor.

4) Actualize sistemas e aplicações
A Microsoft Security Report (2025) indica que a maioria das vítimas usava *software* desactualizado.

5) Use palavras-passe fortes e únicas
E um gestor de senhas. Evite reutilizar credenciais.

6) Eduque a família e a equipa
Idosos e adolescentes são alvos preferenciais. Partilhe sinais de alerta e simule cenários.

7) Reveja movimentos bancários e configure alertas
Rapidez é tudo na contenção de fraude.

Há, contudo, um ponto que merece ênfase: o chamado 'firewall humano' (barreira humana de segurança). Num computador, um *firewall* é uma barreira que filtra tráfego malicioso. No nosso quotidiano, o *firewall* humano é a nossa capacidade de discernimento, atenção e auto-controlo perante pedidos suspeitos. É dizer 'não', é parar para validar, é criar o hábito de confirmar por outro canal. A melhor tecnologia falha sem esta barreira comportamental.

Do lado das instituições, a resposta não pode limitar-se a avisos pontuais. É preciso uma estratégia integrada que una bancos, operadoras, reguladores e forças de segurança. Campanhas continuadas de literacia digital, mecanismos mais claros de bloqueio e reversão de transferências suspeitas, e canais de denúncia rápidos e acessíveis fazem parte da solução. A Europol (Relatório de Cibercrime, 2025) sublinha que organizações que cultivam consciência digital em todos os níveis reduzem de forma significativa as perdas com fraude. A prevenção não é um departamento: é uma cultura.

Formar e proteger: uma nova fronteira. A escalada dos crimes digitais revela uma oportunidade de desenvolvimento profissional em Angola: criar uma carreira específica de polícia de segurança cibernética — investigadores especializados em monitorização, recolha de prova digital e cooperação internacional. Universidades e centros tecnológicos podem lançar cursos e certificações em segurança da informação, resposta a incidentes (incident response), análise forense digital e gestão de risco. As empresas, por sua vez, devem incluir a cibersegurança nos planos estratégicos e nos programas de *compliance*, com métricas e responsáveis claros, simulacros periódicos e formação obrigatória.

Importa lembrar a dimensão humana desta realidade. Ser vítima de fraude digital não é apenas um prejuízo financeiro: é uma ferida emocional. Medo, culpa, vergonha e ansiedade são comuns após o golpe. Como *life coach* e terapeuta, vejo o impacto que um episódio destes pode ter na confiança pessoal e nos relacionamentos. Por isso, a resposta deve incluir apoio psicológico e um roteiro prático de recuperação: contactar o banco, registar queixa, mudar senhas, activar MFA, rever autorizações em *apps*, informar contactos de que a conta foi comprometida.

Casos práticos ajudam a fixar comportamentos. Imagine que recebe uma mensagem da 'sua filha' a dizer que mudou de número e precisa de dinheiro 'já'. Protocolo: 1) não transferir; 2) telefonar para o número antigo; 3) se não atender, pedir nota de voz com uma pergunta que só ela saberia responder; 4) reportar o perfil suspeito. Se o 'banco' ligar a pedir OTP, protocolo: 1) desligar; 2) ligar para o número oficial do banco; 3) reportar o ocorrido; 4) alterar credenciais.

A justiça também precisa de ferramentas. Procedimentos ágeis de preservação de prova (*chain of custody*), cooperação com provedores de serviços e prazos definidos para resposta a incidentes são essenciais para responsabilizar criminosos e desincentivar novas tentativas. Sem consequência, o crime floresce.

No fim, a mensagem é simples: vivemos conectados, mas nem sempre conscientes. Proteger-se digitalmente é um acto de amor-próprio e de responsabilidade colectiva. Se cada um de nós aprender a desconfiar do que parece 'demasiado urgente', a validar o que recebe e a partilhar conhecimento com os outros, estaremos não só a evitar perdas, mas a construir um país digitalmente consciente. Porque, em última análise, a segurança começa na consciência — e a consciência é o primeiro 'firewall humano' (barreira humana de segurança).

Mais de 70% dos casos de fraude digital em África nascem de engenharia social — engano psicológico

A clonagem de WhatsApp está entre as 3 maiores ameaças digitais no continente, ao lado do *phishing*