KIT DE CIBERSEGURANÇA PARA DEPUTADOS E GABINETES PARLAMENTARES

REGRAS, DICAS E CONSELHOS PRÁTICOS

A segurança da informação dos Deputados e do pessoal dos gabinetes dos grupos parlamentares é uma preocupação cimeira da Assembleia da República (AR).

As boas práticas dos utilizadores de equipamentos da AR contribuem decisivamente para este objetivo. Na verdade, é nesta conjugação de esforços que reside a chave de uma política de segurança da informação bem-sucedida.

Com o propósito de ajudar Deputados e grupos parlamentares a protegerem a sua informação, assim como a da AR, reunimos neste documento um conjunto de boas práticas e cuidados relevantes a ter em termos de cibersegurança.

CUIDADOS ESSENCIAIS

- ***PHISHING***
- **COMUNICAÇÕES SEGURAS**
- **PALAVRAS-PASSE FORTES**
- **REDES SOCIAIS**
- **PROTEÇÃO DE EQUIPAMENTOS**

ASSEMBLEIA DA REPÚBLICA | ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

ASSEMBLEIA DA REPÚBLICA | DIREÇÃO DE TECNOLOGIAS DE INOVAÇÃO
CENTRO OPERACIONAL DE SEGURANÇA INFORMÁTICA

PORQUE É QUE SE JUSTIFICA A PREOCUPAÇÃO COM A SEGURANÇA DA INFORMAÇÃO?

Os Deputados são figuras com elevada exposição pública.

A exposição pública faz aumentar significativamente o risco de ataques cibernéticos.

Tais ataques podem comprometer informação sensível, assim como causar danos reputacionais.

Para reduzir esse risco, é essencial que os Deputados e as respetivas equipas mantenham os seus equipamentos e contas digitais protegidas.

Neste documento poderá encontrar algumas dicas simples, mas que podem fazer a diferença.

CUIDADOS-CHAVE (SÍNTESE)

DE QUE FORMA UM DEPUTADO PODE SER ALVO DE ATAQUES?	A forma mais comum de ataque começa com um SMS ou *email* de *phishing*. **Confirme sempre a autenticidade** dos endereços de *email* que recebe e duvide de mensagens que exijam ações urgentes.
REDES SOCIAIS	**Não partilhe palavras-passe** para permitir o acesso de várias pessoas à mesma conta. Em alternativa, deve configurar uma conta de rede social com mais de um utilizador.
COMUNICAÇÕES SEGURAS E APLICAÇÕES DE MENSAGENS	**Para troca de mensagens profissionais relativas à atividade da AR**, nomeadamente com funcionários parlamentares e membros dos seus gabinetes, use a plataforma *Teams*.
PALAVRAS-PASSE FORTES	**Crie palavras-passe longas**. Use, por exemplo, palavras aleatórias, invulgares ou em diferentes línguas.
PROTEÇÃO DE EQUIPAMENTOS	**Coloque sempre palavra-passe** e PIN (padrão, biométrico ou impressão digital) para desbloquear o seu equipamento e **bloqueie-o** quando se ausentar da área de trabalho, mesmo que por um breve período.
SEGURANÇA DAS SUAS CONTAS MAIS IMPORTANTES	**Ative a autenticação de dois fatores (2FA)** nas suas contas mais relevantes (como a sua conta de *email*), garantindo um nível de proteção acrescida.

DE QUE FORMA UM DEPUTADO OU UM MEMBRO DA SUA EQUIPA PODEM SER ALVO DE ATAQUES?[1]

A forma mais comum de ataque começa com um SMS ou *email* de *phishing* (mensagens que visam enganar o destinatário com vista a obter dados sensíveis do utilizador).

Estes ataques podem surgir de diversas formas, por exemplo:

- Pedidos falsos de reposição de palavra-passe;
- Ligações para páginas falsas de *login*;
- Solicitações suspeitas para o envio ou reenvio documentos.

No entanto, também podem ser recolhidas informações pessoais nas redes sociais, fazendo-se os atacantes passar por entidades confiáveis, para tornar os ataques mais credíveis.

[1] Para saber mais: https://arnet/sites/sg/ASI/Documents/Recursos/Pishing.pdf

FORMAS DE PREVENIR UM ATAQUE DE *PHISHING*

1. Verifique sempre que os anexos ou *links* de *emails*, de SMS ou de mensagens nas redes sociais (como o *Facebook* ou o *WhatsApp*) são fidedignos;

2. Não clique em anexos ou *links* suspeitos;

3. Confirme a autenticidade do endereço de *email* (por vezes, as variações relativamente ao endereço original são de pormenor, acrescendo um hífen ou um ponto), do perfil ou do número de telefone de origem;

4. Não forneça dados sensíveis — pessoais ou profissionais — nem siga instruções sem verificar a veracidade do pedido noutras fontes (por exemplo, junto do gestor de conta do banco);

5. Desconfie de mensagens com erros formais de escrita, mas também não confie nas mensagens apenas porque não apresentam estas incorreções;

6. Muito importante: **duvide da credibilidade** de mensagens que exijam ações urgentes;

7. Não partilhe dados sensíveis nas redes sociais, tornando-os acessíveis a possíveis atacantes que queiram realizar o chamado *spear phishing* (*phishing* dirigido a uma determinada pessoa).

No caso de suspeitar de uma situação de *phishing*,
denuncie a situação junto do helpdesk da DTI ou do ASI.
helpdesk@ar.parlamento.pt | ext: 11888 | ASI.Correio@ar.parlamento.pt

REDES SOCIAIS[2]

As redes sociais são um meio de comunicação incontornável, nomeadamente para a mensagem política.

Sem prejuízo da sua importância, o respetivo teor pode ser usado para possíveis ataques, que são cada vez mais sofisticados.

O conteúdo das redes sociais é visto não apenas por amigos, mas por uma vasta audiência que nem sempre se conhece.

Isto é particularmente válido no caso de figuras públicas, como os Deputados.

[2] Para saber mais:
(https://arnet/sites/sg/ASI/Documents/Recursos/Sites%20externos%20redes%20sociais.pdf)

ALGUNS CUIDADOS BÁSICOS A TER NESTAS SITUAÇÕES

A palavra-passe da AR nunca deve ser utilizada em qualquer outro sistema ou *site* externo, incluindo redes sociais;

O *email* da AR não deve ser utilizado no registo em *sites* ou aplicações externas à AR;

Não partilhe palavras-passe para permitir o acesso de várias pessoas à mesma conta (prática comum, por exemplo, na gestão de redes sociais de políticos). Uma vez partilhada a palavra-passe, não há maneira de controlar quem tem acesso à conta. Em alternativa, deve configurar-se uma conta de rede social com mais de um utilizador;

No caso das redes sociais, importa ter presente que as informações pessoais partilhadas podem ser usadas por cibercriminosos, para dar credibilidade a um *email* de *phishing*, por exemplo;

Reveja regularmente as definições de privacidade destes *sites*. Caso não esteja totalmente confortável, opte pela alternativa mais protegida, isto é, aquela em que a partilha de informação é menor.

COMUNICAÇÕES SEGURAS E APLICAÇÕES DE MENSAGENS

Nem todos os meios de comunicação através de mensagens oferecem o mesmo nível de segurança.

Dependendo da natureza da comunicação, use as aplicações mais adequadas e confiáveis.

CUIDADOS A TER

Para troca de mensagens profissionais relativas à atividade da AR, nomeadamente com funcionários parlamentares e membros dos seus gabinetes, a forma mais segura de comunicação é através da plataforma *Teams* (incluída no Office 365);

Nas restantes comunicações, recomenda-se que **opte por aplicações com criptografia de ponta a ponta** (é o caso, por exemplo, do *Signal*, do *WhatsApp* ou do *Telegram*, em modo secreto);

Mesmo quando esteja a usar aplicações fidedignas, **verifique sempre quem está incluído em grupos** (em grupos grandes nem sempre é fácil controlar quem tem acesso à informação);

Nunca é demais o **cuidado** com a informação partilhada em conversas em grupo;

Não abra *links* e arquivos desconhecidos;

Tenha presente que amigos também podem ser vítimas de ataques – devendo, por isso, **desconfiar de mensagens incomuns ou fora do contexto**;

Mantenha as aplicações sempre atualizadas.

PALAVRAS-PASSE FORTES[3]

Palavras-passe fracas podem ser adivinhadas com facilidade, permitindo o acesso à sua informação mais sensível, assim como à da AR.

A Política de Uso Aceitável do Sistema Informático AR (PUA) contém regras importantes sobre o bom uso das credenciais pelos seus utilizadores:

Login e palavra-passe constituem **informação sensível e pessoal**, não devendo ser escritas, enviadas ou guardadas de forma desprotegida;

As credenciais **não devem ser partilhadas** com ninguém;

Em circunstância alguma deve a palavra-passe ser utilizada em qualquer outro sistema ou site externo;

O *email* da AR também **não deve ser utilizado no registo em sites ou aplicações externas à AR**, salvo exceções muito pontuais relativas a soluções ou eventos diretamente relacionados com o trabalho parlamentar.

[3] Para saber mais: https://arnet/sites/sg/ASI/Documents/Recursos/Passwords.pdf

ESCOLHER UMA PALAVRA-PASSE FORTE

Crie palavras-passe longas (por exemplo, com 15 carateres) e inclua uma combinação de letras maiúsculas e minúsculas, números e símbolos;

Uma boa forma de o fazer é criar uma frase de código — frase que inclua **palavras invulgares** ou **palavras em diferentes línguas**;

Outra opção é criar uma palavra-passe através de **três palavras aleatórias**, facilitando a sua memorização;

Tenha em mente que os **cibercriminosos tentam decifrar as palavras-passe mais comuns** (por exemplo, *password1*, datas de aniversário ou nome de familiares) ou usar informações publicamente disponíveis para tentar aceder às suas contas;

Atente que, no caso de serem bem-sucedidos, os **cibercriminosos podem usar a palavra-passe decifrada para aceder às suas outras contas**, razão pela qual é tão importante utilizar uma palavra-passe diferente para a conta de trabalho e outra para cada conta *online*);

Lembre-se que, na eventualidade de se esquecer da sua palavra-passe, **o *helpdesk* da DTI poderá sempre redefini-la, se necessário.**

PROTEÇÃO DE EQUIPAMENTOS

A proteção dos equipamentos (*desktops*, portáteis, *smartphones*, telemóveis ou *tablets*) depende também dos constrangimentos que se coloquem ao seu acesso.

Conheça aqui ao lado práticas simples, que podem evitar que cibercriminosos explorem vulnerabilidades dos seus equipamentos e da sua informação mais sensível.

CUIDADOS BÁSICOS

Coloque sempre palavra-passe, PIN (padrão, biométrico ou impressão digital) para desbloquear o seu equipamento;

Bloqueie o equipamento quando se ausentar da área de trabalho, mesmo que por um breve período;

Quando possível, **ative o "Encontrar dispositivo"** no seu equipamento;

Configure a opção de **apagar dados remotamente** em caso de roubo ou perda;

Mantenha as atualizações de *software* e do sistema operativo em dia (novas vulnerabilidades são identificadas diariamente, que os fabricantes corrigem através das atualizações);

Qualquer perda, extravio, roubo, furto ou avaria de equipamento deve ser reportado, de imediato, ao *helpdesk* da DTI.

SEGURANÇA DAS SUAS CONTAS MAIS IMPORTANTES[4]

A proteção das suas contas mais importantes depende também dos constrangimentos (simples, mas eficazes) que se coloquem ao seu acesso.

A rapidez com que se reaja a situações de quebra de segurança, ou de risco iminente de que isso aconteça, também pode ser um fator decisivo.

[4] Para saber mais, consulte os folhetos informativos disponíveis na área da Administração de Segurança da Informação: https://arnet/sites/SG/ASI/Paginas/default.aspx

CUIDADOS BÁSICOS

Ative a autenticação de dois fatores (2FA) nas suas contas mais relevantes (como a sua conta de email). Isto garante um nível de proteção acrescida, ao enviar, por exemplo, um código PIN para o seu telemóvel na primeira vez (ou sempre, se preferir) que iniciar sessão a partir de um novo dispositivo.

Solicite de imediato o bloqueio da sua conta ou do acesso ao email, no caso de achar que alguma delas (ou ambas) se encontra comprometida.

Se precisar de ajuda, não hesite em pedir o apoio do *helpdesk* da DTI.