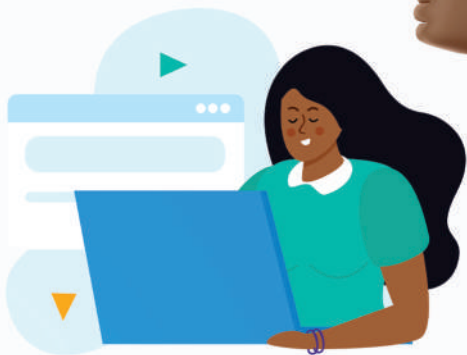


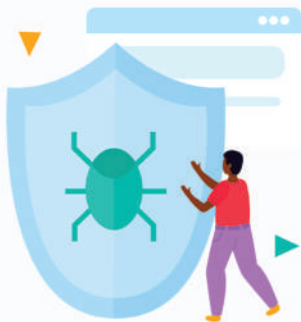
BOAS PRÁTICAS E RECOMENDAÇÕES DE SEGURANÇA CIBERNÉTICA

– GETIN/DIAFI/EMATER-RO –



Não escreva seu login e senha da EMATER-RO em nenhum outro sistema, próprio ou de uma empresa privada. Essa prática é um incidente de segurança.





Números e caracteres não devem ser usados para substituir letras em palavras reais facilmente encontráveis em dicionários. Deve-se, portanto, evitar por exemplo: 3l3f4nt3 (elefante), 30r3013t4 (borboleta), @vestru5 (avestruz), p!an!sta (pianista), etc

Não emprestar sua senha para ninguém, nem para alguém de sua confiança, pois não há como ter certeza de que o computador que será usado está livre de malwares (softwares maldosos)





Observar sua estação de trabalho, verificar se não possui dispositivos keyloggers físicos (pequenos dispositivos que parecem pen drivers) conectados nas portas USB – principalmente a do teclado (estes dispositivos monitoram, coletam e enviam tudo que é digitado e enviam via Wi-Fi).

Não utilizar dados e informações pessoais em senhas, pois são informações que podem ser descobertas por alguém que detenha certas habilidades e permitir a invasão de sistemas do EMATER-RO e de parceiros. Por exemplo: nomes de parentes, nomes de outras pessoas, atividades que você realiza, lugares que você conhece.





**Não usar regras de criação de senhas que sejam fáceis de adivinhar. Por exemplo:
qwertyuiop1010,
qwertyuiop5353.**

Não usar senhas fáceis de descobrir: Por exemplo - 1N551n55 (EMATERroTER), De2eMbr02021 (dezembro2021), etc.





Procurar sempre usar senhas fortes que não sejam repetidas e que estejam sempre seguras.

**Não reutilizar senhas pessoais
(de lojas, bancos, e-mail,
redes sociais) nos sistemas
corporativos, pois se uma senha é
descoberta, outros sistemas
podem ser acessados.**



XXXXX



Ao criar senhas não usar números que sejam fáceis de descobrir, como datas, números sequenciais, repetição de números já usados, números de telefones, de residências, de matrículas, de documentos, etc.

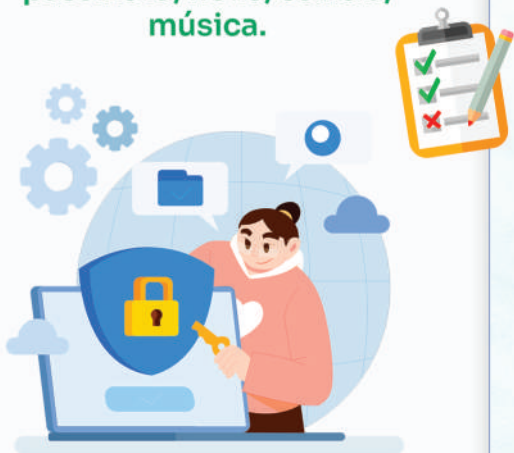
Ao criar senhas não use o método de números sequenciais, como chocolate0001, chocolate0002, chocolate0003, ou ainda, Felicidade123123, Felicidade456456.





O computador tem que estar protegido contra malwares, com o uso de um software antivírus, que deverá estar sempre atualizado.

Evitar o uso de palavras comuns,
já se sabe que as palavras mais
usadas no país ao se criar senhas
são: família, senha, sucesso,
password, novo, estrela,
música.

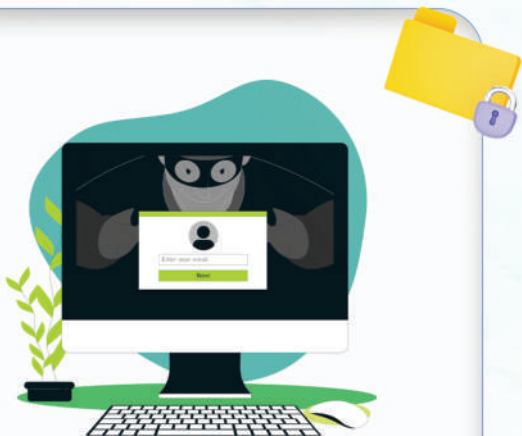




Não permitir que pessoas estranhas ao seu trabalho acessem o computador e sempre que se distanciar dele, deixe-o bloqueado.

Não permitir o acesso remoto a seu computador e caso tenha que fazer isso libere o acesso somente quando for necessário e ao final da sessão remota, certificar-se que o aplicativo não está mais ativo.





Não compartilhar seu computador com terceiros e caso tenha que fazer isso, certificar-se que os outros usuários não acessem seu perfil, muito menos seus arquivos.

Evite se distrair ao acessar os sites da EMATER-RO ou sistemas de terceiros, preste atenção em endereços de Internet que podem ser falsos, que se fazem passar pelo site original, mas estão apenas querendo capturar sua senha.





Evite o uso de softwares piratas

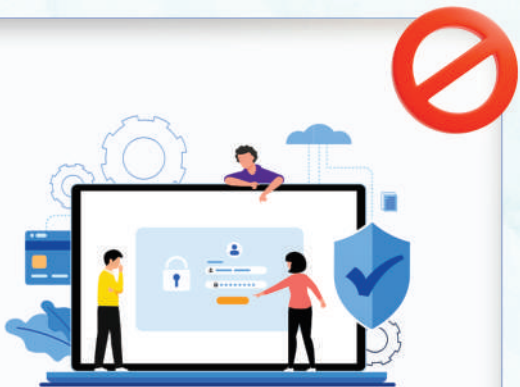


Reforce sua segurança cibernética, observando às melhores práticas de Segurança da Informação.

- **Atualizar seu sistema operacional rotineiramente.**
- **Nunca gravar senhas de forma alguma no seu computador.**

- Fazer backup de seus arquivos em um HD externo (disco rígido externo). Se precisar utilizar redes sem fio para acesso à Internet sempre o faça em uma rede segura.
- Em ambientes públicos ou em ambientes desconhecidos, priorize a utilização da rede 3G, 4G ou 5G do telefone celular.





Qualquer acesso aos sistemas da EMATER-RO ou de terceiros feitos de forma automatizada (robô, ou script de automatização) poderá ser considerado Incidente de Segurança e acarretará bloqueios das credenciais de acesso e do endereço IP usado no acesso à Internet.

Como regra geral, nunca confie em links contidos no corpo de mensagens de e-mail.



Tenha cuidado com os e-mails que receber. Observar se não possuem indícios de fraude, ou tentativa de furto de informação, por exemplo: ortografia imprecisa, termos mal traduzidos, propostas de ganhos extraordinários, ameaças muito agressivas de entidades financeiras, ou fornecedores de serviço. ou solicitações que exigem ação imediata (mudança de senha, instalação de aplicativos, clique em links, promoções, pechinchas, oportunidades de ganho financeiro, etc.).



Em caso de dúvida, sempre consulte o administrador de rede, a área de infraestrutura ou segurança (GETIN) da EMATER-RO e verifique cuidadosamente o endereço de e-mail do remetente. Verifique sempre se não é um Spam, Ransomware, Malware ou Phishing.



MATENHA SEU COMPUTADOR SEGURO DE INVASÕES

