Mantendo sua organização segura online

Por que a segurança cibernética é importante para grupos comunitários e organizações?

Esta página contém conselhos e algumas medidas que você pode seguir para proteger seu grupo comunitário ou organização contra ameaças à segurança cibernética. Há também um guia separado para que as pessoas se mantenham seguras online.

Estes conselhos são baseados nas ameaças mais comuns e graves.

- Atualizações – mantenha o software de seus dispositivos atualizado para corrigir quaisquer falhas na segurança.
    - Mantenha os dispositivos do seu grupo comunitário ou organização atualizados. Isso inclui telefones, computadores, roteadores de Wi-Fi e qualquer outro equipamento que se conecte à internet – incluindo dispositivos inteligentes.
    - Habilite as atualizações automáticas sempre que possível.
- A autenticação de dois fatores (2FA) – adiciona segurança extra às suas contas, exigindo uma etapa adicional além da senha, como um código de um aplicativo em seu telefone.
    - Nota: Isso também é chamado de autenticação multifator (MFA), verificação em duas etapas (2SV) entre outros nomes.
    - Ative o 2FA em todas as contas do seu grupo comunitário ou organização.
    - Se possível, tente usar uma forma de 2FA que seja resistente a phishing, para que você não seja enganado a fornecê-la. Pode ser uma chave de segurança física ou algo como uma impressão digital ou identificação facial.
- Acompanhe suas contas online – certifique-se para que os antigos membros não mantenham acesso às contas após terem deixado o grupo comunitário ou organização.
    - Se houver mais de uma pessoa acessando a mesma conta, certifique-se para que todas possuam logins diferentes e que tenham o 2FA ativado.
    - Mantenha uma lista de todas as contas de usuários e desative as que não são necessárias, como quando alguém da equipe deixa a organização.
    - Mantenha um registo de todos os dispositivos que tenham sido fornecidos aos seus membros e lembre-se de recuperá-los e de restaurá-los para as configurações de fábrica caso essa pessoa deixe a organização. Também pode ser necessário alterar códigos físicos de acesso ao edifício.
- Verifique quem tem acesso às suas contas online – as pessoas do seu grupo comunitário ou organização só devem ter acesso ao necessário.
    - Se a conta de uma pessoa for hackeada, esses passos limitam os danos que um invasor pode causar.
    - Verifique e remova regularmente as permissões desnecessárias.

    - Se uma única conta de "administrador" for usada por várias pessoas, monitore-a em busca de atividades incomuns. Tente limitar este tipo de contas, especialmente para tarefas diárias.
    - Essas regras também se aplicam ao acesso de administrador a dispositivos, como roteadores.
- Revise seus contratos com provedores de serviços – caso tenha contratado alguém para executar serviços de TI.
    - Certifique-se de que eles possuem proteções de segurança cibernética em vigor para atender às necessidades do seu grupo comunitário ou organização.
- Saiba como todas as suas contas e sistemas funcionam juntos – entender essas conexões ajuda a saber por onde um invasor pode ter acesso.
    - Avalie as conexões entre seus sistemas, por exemplo, e-mail, armazenamento na nuvem e plataformas de contabilidade.
    - Considere usar uma Rede Privada Virtual (VPN) para maior segurança online. O uso de uma VPN oculta suas atividades online de qualquer um que tente rastreá-lo. Essa é uma ótima opção, especialmente se algum membro do seu grupo comunitário ou organização estiver usando uma conexão remota.
- Mantenha seu pessoal "ciberseguro" – pessoas são alvos mais comuns do que sistemas.
    - Treine toda a equipe em segurança cibernética básica. O site Own Your Online Own Your Online | NCSC tem uma variedade de conselhos e dicas para ajudá-lo a se manter seguro online e a identificar fraudes.
    - Lembre-os de que estas ações são importantes tanto para suas contas pessoais como para as usadas em sua organização.
    - Também temos um guia para que as pessoas se mantenham seguras online.
- Se prepare para um incidente – ter um plano de resposta ativo é importante para evitar que as pessoas entrem em pânico quando um incidente acontecer.
    - Um plano de resposta determina quem é o responsável por cada ação no caso de um incidente. Há modelos disponíveis aqui Gestão de Incidentes | NCSC
    - Inclua um plano sobre o que fazer caso telefones, computadores ou outros sistemas falhem. Mantenha este plano atualizado.
    - Mantenha os dados de contato de todas as pessoas necessárias e informações alternativas de contato, caso o principal meio de comunicação com elas seja interrompido (como o e-mail).
    - Mantenha o plano em algum lugar fora do seu sistema também, caso você não consiga acessá-lo.