Image not found or type unknown

Planejando comunicações móveis para ações/organização [atividade práticas]



Abaixo apontamos considerações de orientação para grupos que estão se organizando e participando de ações utilizando aplicativos de mensagens. Usando esta guia, você pode facilitar discussões para ajudar grupos a refletirem sobre como são suas formas de comunicação e fazer o design de protocolos de gerenciamento de grupos, mensagens e de dispositivos que atendam às necessidades de segurança dessa comunicação.

Esta atividade conta com 3 estágios:

- Mapeamento de comunicações e avaliação de riscos
- Planejamento: fazer um design de grupos e configurações
- Instalação de Aplicativos (opcional)
- Implementação (opcional)

Se os grupos não tiverem escolhido ainda qual aplicativo de mensagens querem usar, você pode fazer a atividade Discussão, interações + mão-na-massa: Escolhendo aplicativos móveis

Objetivos de aprendizagem aos quais esta atividade responde

- trocar e praticar estratégias e táticas de segurança em telefones celulares para que possamos gerenciar os impactos das comunicações via telefonia celular entre nós, nossas colegas e nossos movimentos;

Para quem é esta atividade?

Esta atividade é para participantes com variados níveis de experiência em usar telefones celulares. Se entre as participantes tiver pessoas que serão administradoras dos grupos de mensagens, planeje implementar os projetos na própria oficina.

Tempo estimado

Esta atividade requer cerca de **60 minutos** para o mapeamento e projeto e até 3 horas se você irá instalar os aplicativos de mensagens, mapear, projetar e implementar o projeto.

Recursos necessários para esta atividade

- Papel para as pessoas fazerem o design de seus projetos e completarem o mapeamento

Dinâmica

Mapeamento de comunicações e avaliação de riscos

Consideração: Privacidade

Considere que você pode ter diferentes tipos de mensagens para comunicar por meio do Signal e que algumas mensagens são mais públicas do que outras. Mapeie os tipos de comunicação que você faz e faça o design de grupos de acordo com suas considerações de privacidade.
Que tipo de comunicação você está fazendo e quais considerações você tem sobre quem tem acesso à comunicação? Sugira que as participantes considerem esses diferentes grupos. Pergunte se elas têm mais tipos de informações - por exemplo, há informações que apenas 2 pessoas devem saber, que apenas uma pessoa deve saber e documentar e não compartilhar?

QUEM	EXEMPLO DE COMUNICAÇÃO

1 precisa ser mantida entre um grupo bem pequeno de pessoas que se conhecem entre si	*localização das principais organizadoras*

2 é vital que as voluntárias saibam ou que pequenos grupos se coordenem	*mudanças na localização da multidão*

3 pode ser compartilhada abertamente	*hora de início da manifestação, grupos que endossam esta ação publicamente*

Planejamento: design de grupos e configurações

Trabalhe com as participantes para fazer o design de grupos que correspondam aos diferentes tipos de comunicação.

Sugestões de orientação sobre o design do grupo: Sugerimos começar com estas questões de design. Incluímos sugestões de exemplo para o gerenciamento de grupos e configurações para alguns tipos mais comuns de grupos. Pergunte às participantes o que vai funcionar e o que não vai para elas, facilite a modificação dos designs dos grupos para melhorar as partes que não funcionam.

Membros

- QUEM – Quem pode entrar neste grupo?
- COMO – Como as pessoas entram neste grupo? Qual o procedimento? Elas precisam ser avaliadas, apresentadas, são inseridas automaticamente, ou se inscrevem?
- RECONHECIMENTO - Como o grupo reconhece quando uma pessoa se junta? Por que você gostaria que o grupo fizesse isso ou não?

- ACORDOS – O que você faz se alguém entrar sem seguir os procedimentos?
- INFORMAÇÕES PESSOAIS - com o serviço de mensagens que você está usando, membros do grupo podem ver os números de telefone de outras do grupo? Nesse caso, para quem precisa que seu número não seja conhecido como parte da organização, não deve se juntar a nenhum grupo grande em que as outras pessoas ainda não saibam seu número e que a pessoa faz esse trabalho.

Saiba com quem você está falando - VERIFICAÇÃO

Para cada tipo de comunicação, como você irá verificar com quem você está de fato falando?

- CARA-A-CARA - você exigirá que algum membro do grupo encontre o resto do grupo cara a cara para ingressar? Uma pessoa pode simplesmente ser adicionada e certificada por um membro do grupo?
- Nºs DE SEGURANÇA - VERIFIQUE se suas mensagens estão indo para os dispositivos corretos. Se você estiver usando Signal ou WhatsApp, VERIFIQUE OS NÚMEROS DE SEGURANÇA
- PALAVRAS DE SEGURANÇA - VERIFIQUE se suas chamadas estão indo para os dispositivos corretos. Se você estiver usando o Signal para chamadas, FALE AS PALAVRAS DE SEGURANÇA com a pessoa que deseja falar. Se você estiver usando outro aplicativo de chamadas, pense se quer ter uma maneira de fazer check-in no início de uma chamada para verificar se a pessoa é quem você pretendia e está falando livremente.

Segurança de mensagens - configurações

Discuta, com base na sensibilidade das informações que você está comunicando, que tipo de acordos você deseja fazer sobre como as pessoas estão usando as configurações de mensagens. Por exemplo:

- DELETAR Mensagens - Por quanto tempo os membros do grupo devem manter logs de bate-papo em seus dispositivos?
- Mensagens EFÊMERAS - Em um chat do Signal, você pode definir quanto tempo as mensagens permanecerão antes de serem excluídas automaticamente. Você quer usar este recurso? Como e por quê?
- OCULTAR mensagens na tela inicial - Configure os aplicativos de mensagens para não serem visualizados na tela inicial, de modo que, se você perder o controle do dispositivo,

as pessoas não poderão ver o conteúdo da mensagem na tela inicial.
- CÓDIGOS - Para informações extremamente confidenciais, sugerimos estabelecer palavras-código antes de planejar e agir. Por exemplo, você pode substituir as palavras "Estamos prontos para a festa do chá" em vez de "Prontos para o protesto!"

Modelos de design para grupos

1. Pequenos grupos altamente verificados para informações confidenciais

> Consideração/risco: que as pessoas entrarão em grupos desconhecidos e que não sabem se as informações lá veiculadas podem ser publicizadas ou não.

- Se você tiver informações confidenciais que precisam ser compartilhadas apenas entre um conjunto de pessoas conhecidas;
- Grupo muito pequeno, 8 ou menos, todos se conhecem e se encontraram cara a cara;
- Adicione pessoas apenas quando estiver cara a cara;
- VERIFICAR Identidade (no Sinal, verificar Números de Segurança) pessoalmente;
- Se o número de segurança de alguém mudar, verifique novamente pessoalmente;
- Não diga mais do que o necessário, não corra riscos desnecessários;
- DELETE

2. Células - grupos de trabalho reduzidos

> Consideração/risco: Que as pessoas se juntem ao grupo e enviem informações que não sejam úteis ou intencionalmente incorretas.

- Desta maneira, diminui o risco de indivíduos enviarem spam para um grande grupo e torná-lo inutilizável e cheio de ruídos;
- Grupo de 2 a 20 pessoas, o que for necessário para se manter o número de mensagens baixo e ter um número gerenciável de células no Signal;
- Um grande grupo pode ter várias células para manter a comunicação gerenciável e relevante;

- As células são conectadas umas às outras para que as informações possam fluir entre elas. Você pode considerar ter uma pessoa-chave em cada célula para que elas possam enviar informações que todos precisam ter.

3. Grupo aberto, informação pública

Considere as informações neste canal como informações públicas em tempo real. Embora as informações de qualquer um dos outros grupos possam vazar ou ser compartilhadas fora do grupo, este é um grupo que você automaticamente considera público.

- Se você tiver alguma informação para compartilhar que possa ser tornada pública, use este modelo!

Segurança do dispositivo

Se o seu dispositivo for levado, evite que outras pessoas finjam ser você e leiam suas informações, como mensagens de sinal, catálogo de contatos, e-mail, etc. Para orientações de facilitação mais detalhadas sobre segurança de dispositivos, consulte a atividade: Faça Back-up! Bloqueie! Delete! a.k.a. Alguém pegou meu celular: Roubo, encarceramento, acidente, cruzar fronteiras.

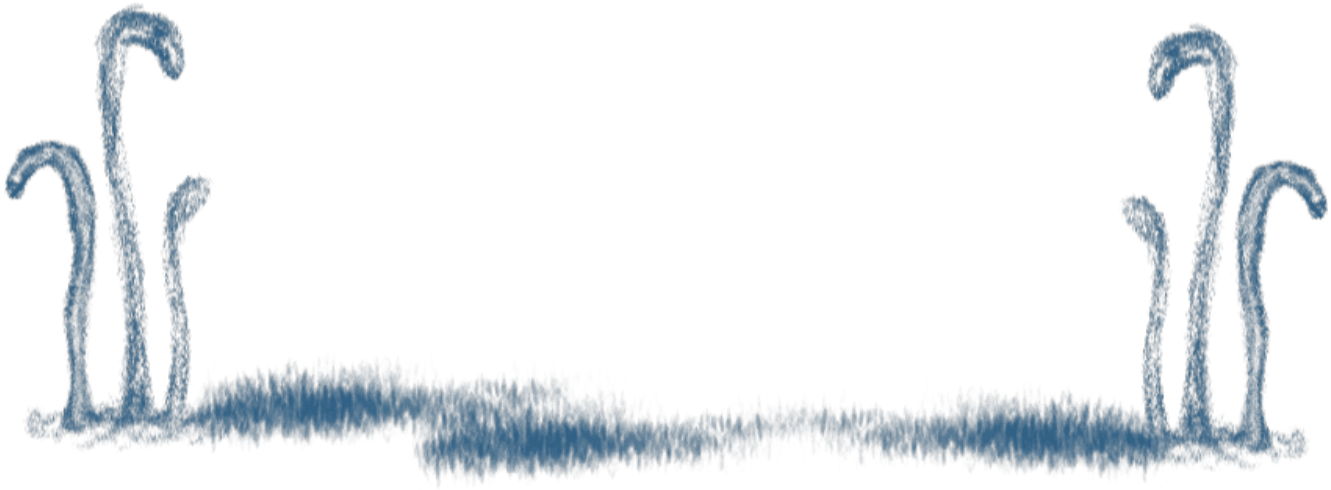
- Defina um bloqueio para imediato que possa ser disparado facilmente
- Tenha uma senha forte
- Criptografe seu telefone
- Criptografe seu cartão SIM

Energia e serviço

E se as pessoas não puderem usar Signal ou outros aplicativos específicos, telefones, Internet, por qualquer motivo - energia, rede ocupada, desligamento etc. Você tem backup ou acesso redundante à Internet - um hotspot de wi-fi portátil, por exemplo (se ele usa dados de celular isso também diminuiria)? Existe um plano offline? Seu hub terá uma estação de carregamento de energia para voluntários?

Recursos adicionais

- Sobre como verificar Números de Segurança e Palavras de Segurança [em inglês] - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/



Revision #5
Created 26 April 2023 01:41:27 by Kira
Updated 28 July 2023 15:05:17 by Kira