Segurança em Mídias Sociais

SETISD – HC-UFG

ELABORAÇÃO

Johnathan De Palma Lopes – Chefe da Unidade de infraestrutura , Suporte e Segurança da Tecnologia da Informação
Ricardo Oliveira Macêdo – Técnico de informática
André de Oliveira Penna – Analista de Tecnologia da Informação
Evatir Rezende De Barros – Chefe da Unidade de Sistemas de Informação e inteligência de dados
Alisson Bastos Dutra – Analista de Tecnologia da Informação
Glaudine Reis Godoi – Técnico de informática
Fernando Augusto De Azevedo Guimarães – Técnico em informática
Alessandro Carvalho da Fonseca - Chefe do Setor de Tecnologia da Informação e Saúde Digital

Sumário

1 Segurança da informação

Aos colaboradores e familiares do HC-UFG, a SETISD elaborou a presente cartilha sobre Segurança da Informação com o objetivo de orientá-los quanto aos procedimentos a serem adotados para preservar a segurança de suas informações bem como de seus familiares. Numa sociedade cada vez mais digital, se faz necessário um conhecimento prévio na área de segurança da informação para que possamos nos proteger das ameaças constantes no cyberespaço.

3. Sites de redes sociais

As redes sociais são sites na internet que permitem que usuários de diferentes regiões se conectem uns aos outros, compartilhem informações, imagens, vídeos e também conversem.

Rede social é processo de conexão através desses sites:

3. Sites de Redes Sociais / O que é um Perfil

Um perfil é a coleção de informações que define ou descreve o usuário e seus interesses.

Algumas das informações que um usuário pode postar em seu perfil são:

- Nomes / Apelidos
- Fotos / Vídeos
- Interesses pessoais
- Endereço de E-mail

3. Sites de redes sociais / Quais são os riscos associados a sites de redes sociais?

Phishing	É um método de fraude por e-mail em que o agressor envia e-mails legítimos em uma tentativa de reunir informações pessoais e financeiras dos usuários
Roubo de identidade	O roubo de identidade é um ataque no qual os perpetradores personificam suas vítimas e gastam seu dinheiro;
Malware	Malware é um software malicioso que danifica ou assume o controle de um computador ou rouba informações dele;
Falhas no site	Falhas de segurança em sites de redes sociais permitem que invasores acessem e roubem informações do usuário;
Spoofing de URL	É o método de criar URLs falsas que imitam um site legítmo e original para fazer os usuários visitarem sites perigosos;
Clickjacking	É uma técnica de enganar os usuários da web para revelar informações confidenciais ou assumir o controle de seu computador enquanto clica em páginas da web aparentemente inofensivas, por exemplo, facebook Like jacking.

3. Sites de redes Sociais / Quais são os riscos associados a sites de redes sociais?

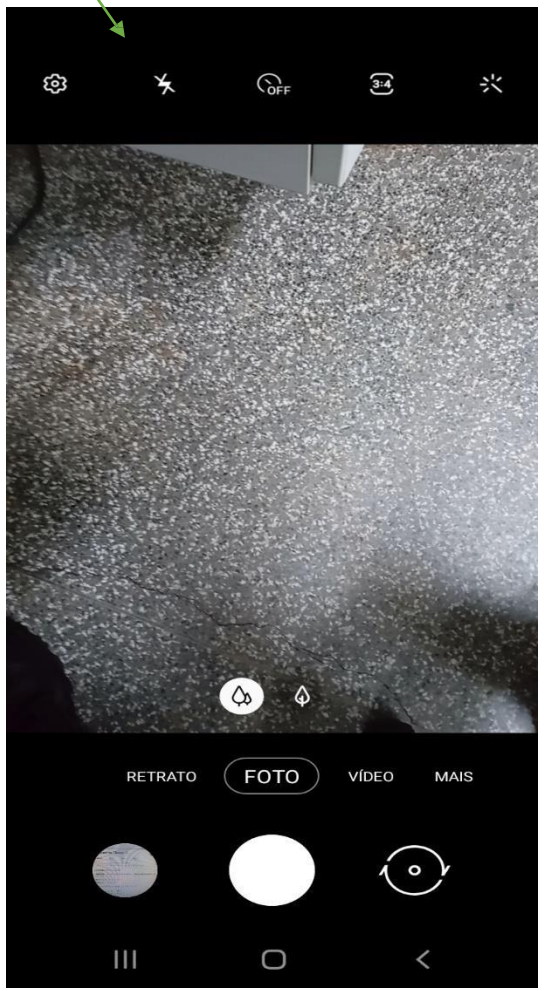
A engenharia social é um método não técnico de uso de hackers por invasão que depende muito da interação humana e, muitas vezes, envolve enganar as pessoas para que infrinjam procedimentos normais de segurança.

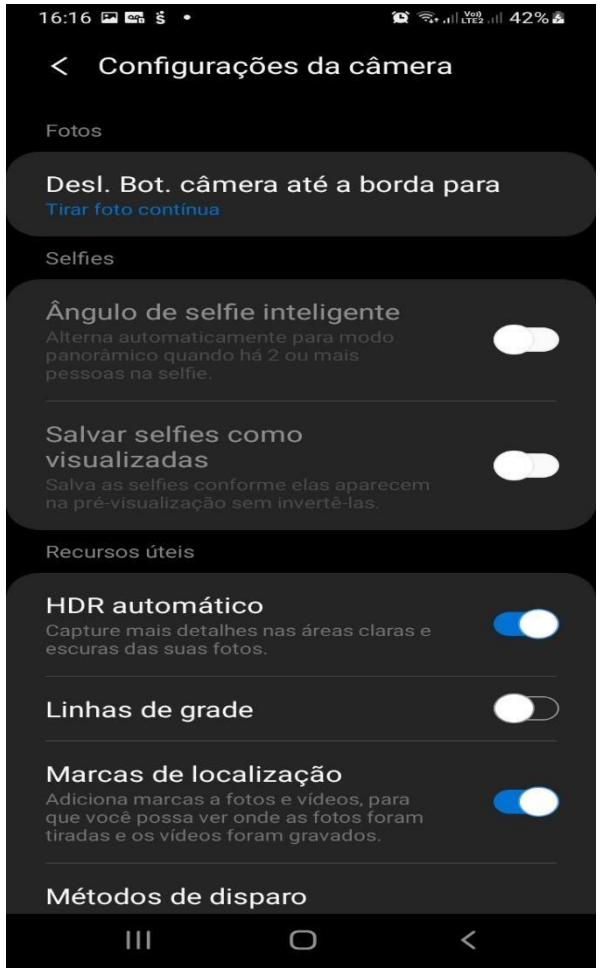
Abordagem direta	É quando as vitimas têm que participar diretamente do ataque para que seja bem sucedido. Nesta abordagem, as vítimas inadvertidamente entregam suas informações como em um e-mail de phishing ou uma chamada de phishing.
Abordagem indireta	Tira vantagem de pessoas que não tem consciência situacional. Os agressores obtém informações por engano sem a participação direta de vítimas como no caso **sholder surfing.**

3. Geotagging

Geotagging refere-se ao processo de adicionar informações geográficas, na forma de latitudes e longitudes, a várias formas de mídia.
Essas informações geográficas especificam onde exatamente uma determinada foto foi tirada ou uma atualização de status específica foi postada;
Uma grande ameaça associada a Geotagging é que ele fornece os locais de você e seus entes queridos para qualquer pessoa que tenha acesso às imagens;
Muitos sites, como o instagram e o Flickr, também fornecem um mapa completo de todos os lugares em que uma pessoa em particular tirou fotos;
Por exemplo, uma jovem que publica fotos dela online ou atualiza um status regularmente pode ser rastreada até um local preciso para descobrir seus movimentos diários por meio de fotos, postagens e tweets como geotag.
Você pode impedir que suas fotos sejam georreferenciadas, desativando o recurso de localização presente nas configurações da câmera em seu telefone.

3. Geotagging





Essa configuração é válida para aparelhos Android

4. Segurança aplicada no facebook

De acordo com os estatísticos do zephoria.com, o facebook tem 1,44 bilhões de usuários ativos por mês, 1.25 bilhão de usuários móveis ativos mensais, 300 milhões de fotos atualizadas diariamente e 20 minutos gastos por visita.

Selecione (filtre) quem pode ser seu amigo

Ajustes as configurações de Privacidade ← **DICAS DE SEGURANÇA DO FACEBOOK** → **Dentre seus círculos de amigos, configure acesso parcial às suas informações a quem você julgar necessário**

4. Segurança aplicada no facebook

Passo 01

Passo 02

Passo 03

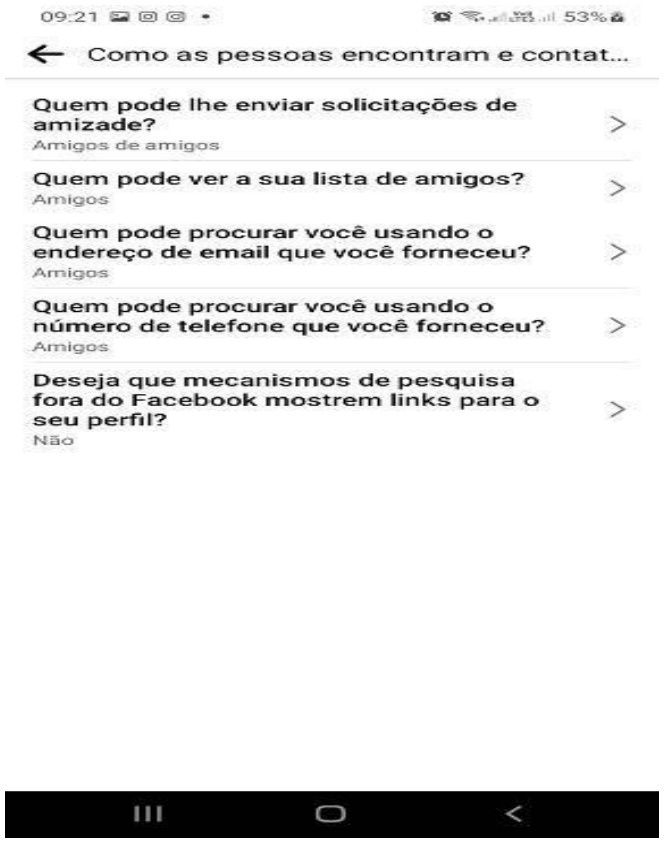
4. Segurança aplicada no facebook

Passo 04

Passo 05

Passo 06

4. Segurança aplicada no facebook



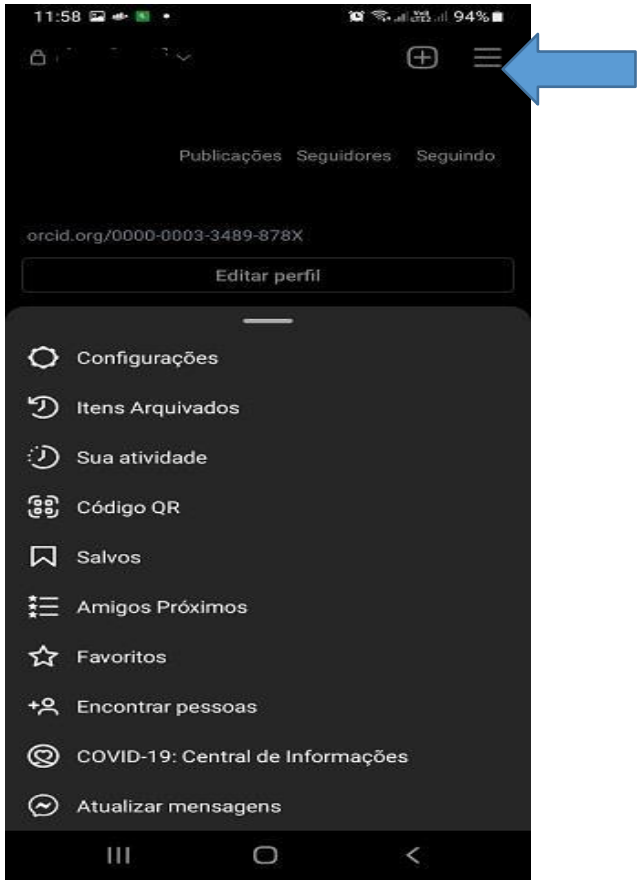
Passo 07

Passo 08

Passo 09

4. Segurança aplicada no facebook

5. Segurança aplicada no Instagram



Passo 01

Passo 02

Passo 03

5. Segurança aplicada no Instagram

Passo 04

Passo 05

6. Segurança infantil online / Quais são as ameaças das redes sociais para menores de idade?

As crianças podem se deparar com mensagens obscenas, fotos explícitas e mensagens de ódio em sites de redes sociais
Pedófilos podem prender crianças fazendo amizade com elas em sites de redes sociais;
As redes sociais carregam o risco de influenciar adolescentes com conteúdo político e religioso. Houve casos no passado em que organizações terroristas recrutavam adolescentes através de redes sociais.

6. Segurança infantil online

Com mais de um trilhão de páginas da Web exclusivas a partir de 2008, as crianças podem ser expostas a uma grande variedade de conteúdos.
Essas páginas da Web têm todo tipo de conteúdo, desde pornografia até doutrinas políticas.
Uma grande parte do conteúdo online não é adequada para ser visualizada por crianças.
Tomar medidas para proteger o conteúdo visto pelas crianças e monitorar sua atividade on-line é o primeiro passo para a segurança delas.

6. Segurança infantil online

Acesso a conteúdo impróprio, como pornografia, mensagens de ódio e fotos explícitas:
Tornando-se vítimas do cyberbullyng;
Predadores online compram nomes de domínio, como o.com equivalente a um popular .gov ou site .org sabendo que os internautas provavelmente acabarão em seu site em vez do destino desejado. Por exemplo, se uma criança está procurando informações sobre a Casa Branca, ele pode encontrar-se em um site pornô em vez do site oficial em www.whitehouse.gov;
Aliciamento é um dos principais riscos enfrentados pelas crianças online. Refere-se a um ato de fazer amizade e estabelecer uma ligação emocional com as crianças, de modo a prepará-las para o abuso infantil;
Pedófilos usam sites de redes sociais e salas de bate papo (às vezes posando como crianças ou adolescentes) para iniciar conversas com as prováveis vítimas.

6. Segurança infantil online / Crianças que sofrem abuso online, apresentam?

Mais tempo que o normal gasto no computador/celular
Presença de material pornográfico em seu computador;
Alternância entre diferentes janelas quando os pais se aproximam;
Recebimento de ligações telefônicas de pessoas desconhecidas;
Parecem deprimidos e perdem o interesse por tudo.

6. Segurança infantil online / Instruções para proteger as crianças contra ameaças online

Garantir que a criança tenha conhecimento sobre ameaças online
Monitorar o uso da criança no computador
Restringir o acesso a conteúdos inapropriados usando um software de filtro de internet
Monitorar o perfil das redes sociais das crianças
Garantir que a criança não forneça nenhuma informação pessoal para estranhos
Notificar a polícia se a criança estiver em contato regular com um estranho

7. Como reportar um crime na internet

Reportar um crime na internet é similar a reportar um crime comum: ele deve ser reportado a uma central de polícia.

8. LGPD X mídias sociais

A LGPD (Lei Geral de Proteção de Dados) começou a valer em setembro de 2020 e trouxe muitas novidades nos procedimentos sobre **segurança e privacidade nas redes sociais**.

Assim, todas as empresas ou órgãos públicos só poderão guardar ou usar dados pessoais com o consentimento expresso dos usuários.

O que são dados pessoais?

Impactos?

O que fazer?

Link para LEI:
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

DÚVIDAS

Em caso de dúvidas sobre a cartilha, entrar em contato com o STISD:

Ramal: 8910