SEGURANÇA DA INFORMAÇÃO PARA TODOS

CARTILHA GERADA A PARTIR DAS PUBLICAÇÕES REALIZADAS PELOS ALUNOS DO PROJETO DE EXTENSÃO SEGURANÇA DA INFORMAÇÃO PARA TODOS DA UNISAGRADO, DURANTE O ANO DE 2021.

UNISAGRADO
Ensino Superior de Excelência

Objetivo do projeto: Conscientizar pessoas e empresas das vulnerabilidades existentes na internet, ampliando e disseminando conhecimentos sobre a importância de conhecer e colocar em prática a segurança da informação.

Objetivo da cartilha: Divulgar em um documento único as publicações realizadas pelos estudantes participantes de projeto. As publicações foram criadas pelos estudantes e orientadas pelo professor responsável do projeto.

Professor responsável pelo projeto: Henrique Pachioni Martins.

Bauru – SP | 2021

SUMÁRIO

PROTEGENDO O SEU APP (SELO DO WHATSAPP)

- → **A verificação em 2 etapas é um recurso opcional no whatsapp!**
- → Ao ativar, qualquer tentativa de uso do seu número de celular (em outros aparelhos e/ou por terceiros) terá que usar, também, um pin de seis dígitos.
- → Você poderá inserir seu endereço de e-mail para caso venha a esquecer o código de acesso. É importante, porém, que a sua conta de e-mail esteja segura.

6 passos para ativar a verificação em duas etapas do whatsapp

1) Com o whatsapp aberto toque no menu de três pontos e acesse as "configurações";
2) Em "conta", escolha "verificação/confirmação em duas etapas";
3) Toque em "ativar" e escolha uma senha seis dígitos para a conta do whatsapp;
4) Confirme o seu pin (digite novamente o seu , código pessoal);
5) Informe um endereço de e-mail válido para caso esqueça seu código;
6) Toque em "avançar" e confirme seu endereço de e-mail, depois em "salvar".

Fique alerta se você receber um e-mail supostamente do whatsapp para desativar a verificação em duas etapas sem ter solicitado, não clique em hipótese alguma.
Outra pessoa pode estar tentando registrar o seu número no whatsapp e invalidar o seu pin.

Para ajudar você a se lembrar do seu próprio pin, o whatsapp irá solicitar que você o digite periodicamente. Não há como desativar essa solicitação que ocorrerá de tempos em tempos sem que a verificação em duas etapas em si também seja desativada.

Prontinho! Após ativar a confirmação em duas etapas, você poderá adicionar seu endereço de e-mail. Isso permite que o whatsapp envie um link para que você possa redefinir seu pin e muda a manter sua conta segura.

Créditos aos estudantes: Welerson Cassamasso Barbe e Lívia Caroline Coelho dos Santos

CUIDADOS COM SEUS E-MAILS

Receber e-mails é algo mais do que comum nos dias de hoje, por esse motivo é necessário tomar cuidado com o que se acredita e estar sempre alerta para possíveis golpes.

Cheque sempre o remetente do e-mail, evite confiar em endereços compostos por números, letras embaralhadas e símbolos, pois pode ser falso, enviado em massa. Em caso de empresas, sempre verifique no site oficial o endereço da empresa que é utilizado para enviar e-mails aos usuários; nunca abra mensagens de pessoas que não conhece, mesmo nesses casos, certifique-se que ela realmente pretendia enviar um e-mail.

Quando receber um anexo, lembre-se se você solicitou por aquilo, se certa cobrança faz sentido e nunca abra antes de ter completa certeza. Tome cuidado com a caixa de Spam do seu e-mail, já que lá se localizam possíveis mensagens não solicitadas ou suspeitas.

Caso abra um link o qual não tem muita certeza de sua origem, procure por erros de digitação, números estranhos e símbolos em lugares aleatórios no nome do site, evite fortemente fornecer seus dados pessoais, porque os mesmos podem ser comprometidos.

Créditos aos estudantes: Carla Kremer de Oliveira e Luis Felipe Paludetto Silva

OS PERIGOS NAS REDES PÚBLICAS DE WIFI

VOCÊ SABIA?

Redes públicas de WIFI podem trazer algumas dores de cabeça se não ficarmos atentos a nossa segurança digital.

Cibe criminosos usam redes públicas de wi-fi de estabelecimentos como hotéis, cafeterias e aeroportos para cometerem seus crimes, roubando dados dos usuários de maneira imperceptível.

COMO FUNCIONA?

→ Cibe criminosos criam um ou mais pontos de redes "falsos" por meio de um equipamento para transmitir um sinal de rede WIFI, onde usuários do estabelecimento encontram a rede aberta.

→ Após usuários se conectarem ao ponto falso da rede, todo tráfego é redirecionado para o computador do Cibe criminoso. Através de ferramentas digitais ele captura todos os dados digitados: e-mails, senhas e até mesmo arquivos de mídia.

COMO SE PROTEGER?

- ✓ Confie apenas em redes WIFI protegidas, ou seja, aquelas que pedem senha.
- ✓ Desligar o WIFI ao terminar de utiliza-lo também é uma forma de proteção.
- ✓ Limpe conexões de redes memorizadas.
- ✓ Ao utilizar uma rede pouco confiável, procure não entrar em sites que necessitem de dados sensível: internet banking, login e compras online com cartão de crédito.
- ✓ O ideal é que, quando não tiver acesso ao uma rede WIFI segura, usar apenas seus dados móveis (4G).

Créditos aos estudantes : Anderson Beloni Clarindo e Keterly Geovana Gouvia Silva

FURTOS DE IDENTIDADE NA INTERNET

Quando uma pessoa tenta se passar por outra com o objetivo de obter vantagens indevidas. Como por exemplo: criar perfis em seu nome ou acessar o seu e-mail e enviar mensagens se passando por você.

Como pode acontecer?

O furto de identidade se torna fácil quando você disponibiliza informações sobre sua vida e sua rotina. Outra forma de coletar informações seria por meio de tentativas de adivinhar as suas senhas, o que se torna fácil se as senhas não forem bem elaboradas. O golpista pode também usar códigos maliciosos para coletar informações suas, que podem chegar até você por meio de conexões não seguras.

Algumas Consequências:
- Perda de reputação;
- Perdas financeiras;
- Falta de crédito.

Como prevenir:
- Evitar exposição de dados pessoais;
- Cuidado ao usar e ao elaborar senhas;
- Cuidados ao se conectar em redes duvidosas.

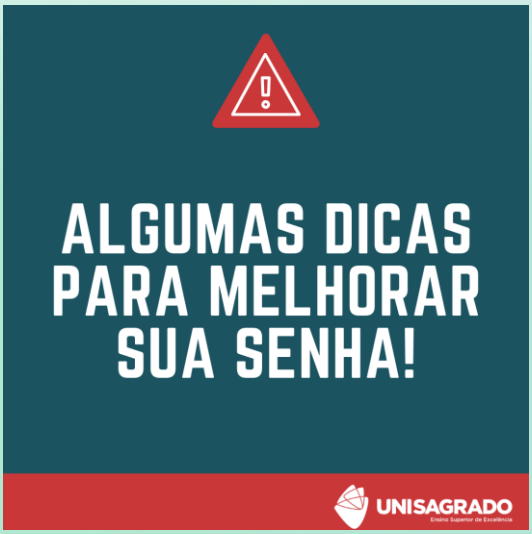
Por fim...

Atente-se se você começar a ter:
- Problemas com órgãos de crédito;
- Receber retorno de e-mails que não foram enviados por você;
- Notificação de acesso em suas redes sociais em horários em que você não acessou;
- Transações bancarias suspeitas;
- Receber ligações e e-mails se referindo a assuntos que você não sabe a respeito.

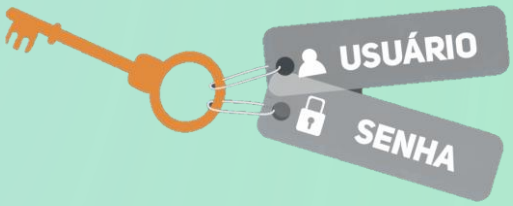
Caso perceba qualquer um desses indícios tome as providencias cabíveis!

Crédito a estudante: Ana Carolina de Oliveira

ALGUMAS DICAS PARA MELHORAR SUA SENHA



- Não use datas, seu nome, nome de algum parente, endereço e/ou sua cidade;



- Não use a mesma senha para todos os sites, redes sociais e bancos;

- Vise utilizar letas maiúscula, minúscula e números, bem como caracteres diferentes (!,@, #, ?);

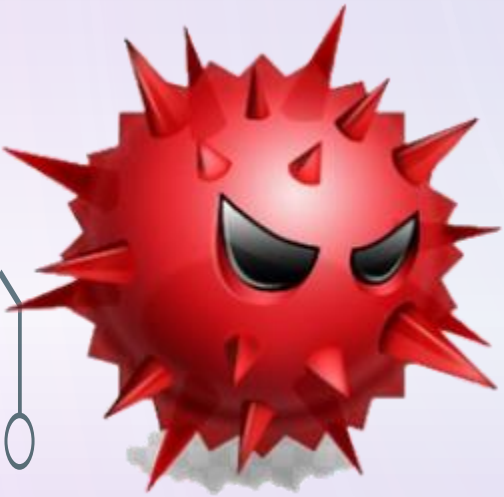
- Tente trocar suas senha pelo menos 1 vez a cada mês.

Crédito ao estudante: Murilo Chiese Leite

ANTIVÍRUS

O que é?

É um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário.



Qual a importância?

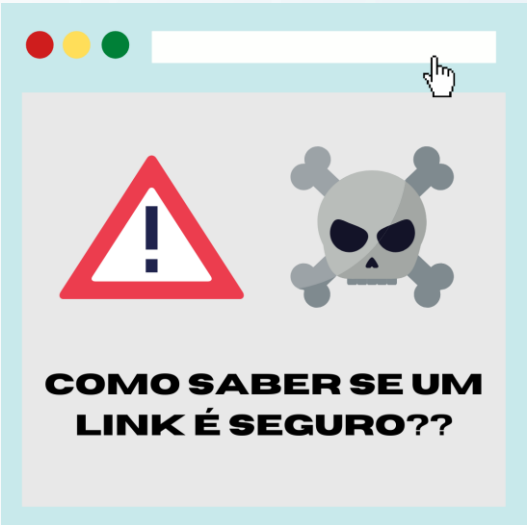
Um antivírus possui rapidez na detecção de vírus e de ameaças virtuais, protegendo e mantendo todas as informações da sua empresa em segurança. Proteja os desktops, notebooks, servidores e todos os dados da sua empresa com um bom antivírus.

É necessário ter antivírus no computador?

Acreditar que um antivírus não é necessário é um mito, especialmente se você é usuário de Windows. Vulnerabilidades nos sistemas operacionais são exploradas por cibe criminosos a todo o momento, e mesmo os usuários mais cautelosos podem cair em golpes bem arquitetados.

Crédito ao estudante: João Gabriel Monteiro Ribeiro

COMO SABER SE UM LINK É SEGURO?



INSTALE UM BOM ANTIVÍRUS

É essencial ter um bom antivírus que proteja sua navegação. Ele pode emitir um alerta já no primeiro contato com ameaças e evitar danos.

www.fac3book.com.br

www.facebook.com.br

LEIA O ENDEREÇO COM ATENÇÃO

Internautas desatentos podem passar despercebido por links sutilmente modificados por criminosos virtuais. Desconfie de caracteres estranhos.

FAÇA UMA CONSULTA ONLINE

http://www.siteadvisor.com/sites/???

Existem ferramentas que verificam se sites são suspeitos. A apresentada acima é gratuita, e basta trocar o "???" pelo site de interesse para verificá-lo.

VERIFIQUE A SEGURANÇA DO SITE

A figura do cadeado ao lado do endereço indica que os dados são criptografados, e o site seguro. Sua ausência é motivo de desconfiança.

Crédito ao estudante: Henrique José de Araujo Junior

ATENÇÃO COM LINKS PERIGOSOS

Mas afinal: o que é URL?

É aquilo que representa um endereço eletrônico de um site, como por exemplo:
https://www.google.com.br
Entenda o que esse endereço significa

https:// - Protocolo de segurança que o site usa
www - (World Wide Web) é uma sigla que representa a internet
google - Este é o domínio do site, ou seja, o site propriamente dito
.com - Representa o tipo de entidade do site sendo
- .com - comercial,
- .gov - governamental,
- .org - organização sem fins lucrativos, entre outros.

.br - O país de origem do site:
- .br - no Brasil,
- .pt - Portugal,
- .jp - Japão, e entre outros

E o que vem após uma barra (/), representa o subdomínio, isto significa, uma parte do site "mãe" como por exemplo: www.facebook.com/Jõao Neste exemplo é o a página do João dentro do facebook

Antes de clicar no link leia com atenção o está escrito Tenha muita atenção no que está escrito no domínio do site, pois é muito comum golpes no qual o criminoso faz uma pequena alteração no nome do domínio como:

fecebook ao invés de fecebook.
rnercadolivre, no lugar de mercadolivre.

Desta forma, redirecionando a vitima para o site do criminoso e não ao site oficial.

Assim que acessar um site suspeito sempre verifique se há, no canto esquerdo do endereço do seu navegador, um cadeado fechado

Ele representa que a conexão com o site é segura e segue os protocolos de criptografia

Crédito ao estudante: Yuri Terração Faria

CONSCIENTIZAÇÃO VOLTADA À ÁREA DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE TRABALHO

1. Bloquear o computador ao se ausentar do posto de trabalho, a fim de que ninguém tenha acesso aos seus dados

Uma medida simples, porém uma proteção para problemas maiores. É como diz o ditado, melhor prevenir do que remediar

2. Nunca disponibilizar logins e senhas, mesmo que para colegas de trabalho

Disponibilizando os dados pessoais para uma pessoa, é necessário ter em mente que ela poderá utiliza-los para o que bem entender

3. Ter atenção ao falar sobre a empresa, clientes ou negócios em ubers, elevadores e metros, por exemplo

Falar publicamente das informações confidenciais de sua empresa, poderá resultar em problemas futuros e prejuízos financeiros, no pior dos casos

4. Verificar atentamente os e-mails

Ataques de pishing estão cada vez mais frequentes, inclusive a sua variável spear pishing, que visa alvo específicos.

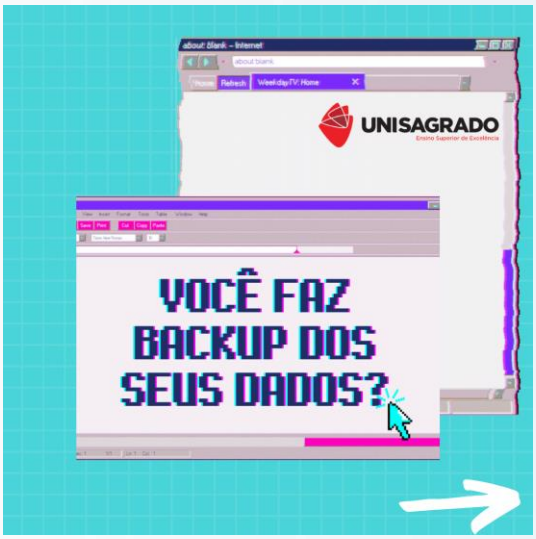
Ao receber um e-mail, é fundamental prestar muita atenção nos conteúdos contidos no mesmo

5. Reportar à equipe de segurança de sua empresa qualquer problema ou desconfiança em relação às atitudes suspeitas na internet

A equipe de segurança de sua empresa deve ser vista como sua maior aliada. Sendo assim, é importante relatar qualquer problema ou suspeita, a fim de que os especialistas analisem o acontecimento, diminuindo as chances de um ataque

Crédito ao estudante: Welerson Cassamasso Barbe

VOCÊ FEZ BACKUP DOS SEUS DADOS?



Backup em mídia física

Neste tipo de backup, a cópia de segurança dos seus dados é feita em dispositivos removíveis, como HDs externos, CDs e pen drives.

Para isso, é realizada a cópia do arquivo no dispositivo que se deseja realizar o backup e é feita a transferência da cópia para uma mídia física.

Lembrando sempre que, o ideal nesse caso, é manter a mídia física em um local seguro, sendo recomendado também a realização da criptografia dos dados armazenados.

O que e Backup?

O backup se trata de uma cópia de segurança dos seus dados salvos em um dispositivo de armazenamento (computadores, celulares, tablets) ou sistema (aplicativos, softwares e jogos) para outro ambiente, com o intuito de que esses mesmos dados possam ser restaurados em caso de perda dos originais.

Ou seja, ele existe para prevenir a perda de dados, como arquivos apagados acidentalmente por falha física ou humana, e é recomendado que seja realizado regularmente.

Backup na nuvem

No Backup na nuvem, você basicamente utilizará um espaço de armazenamento de outro dispositivo e salvará seus dados em um servidor remoto, o qual você irá acessar online, sem precisar de mídia física.

Há vários serviços de nuvem com planos gratuitos como Google Drive, Dropbox, iCloud e OneDrive.

Fazer backups usando estes serviços permite não só manter os arquivos salvos com segurança, como também ter maior facilidade na hora de acessá-los a qualquer momento e em qualquer outro computador ou dispositivo móvel.

Crédito a estudante: Luana Quinaglia Maistro

7 VANTAGENS DE REALIZAR BACKUP EM NUVEM

1. Acesso remoto

O backup em nuvem permite um processo igual dos formatos tradicionais, a diferença é o armazenamento das informações ser remoto e não mais em HDs externos. Não há mais o manuseio direito dos arquivos, tendo um ganho na Produtividade.

2. Acesso remoto

A segurança se da pelo acesso apenas de quem está envolvido no processo.

Terceiros não conseguirão interceptar os dados sem as chaves de segurança.

3. Investimento menor

Do espaço físico, mantendo um funcionário responsável e softwares para a função do backup para serviços remotos apenas com supervisão de um profissional especializado.

4. Foco no negócio

Já que a solução está baseada na nuvem, o backup pode ser contratado como um serviço.

Uma empresa terceirizada fornecerá servidores externos (Data center seguro) e disponibilizará um funcionário para o monitoramento de todos os processos.
Profissional especializado = custo-benefício!

5. Escalabilidade

Basicamente, o contratante do Serviço de nuvem irá pagar apenas pelo que usar (escolha do pacote).

Não precisará adquirir mais equipamentos, basta apenas alterar o contrato.

6. Agilidade

Se os dados estiverem armazenados online, o acesso poderá ser feito a qualquer momento e de qualquer lugar.

7. Segurança

Backups armazenados em mídias tradicionais, onde o risco de roubo e perca desses dados são recorrentes.

Sem a intervenção humana, quando armazenados na nuvem, trazem mais segurança, já que não terá interceptação sem as chaves de segurança.

Crédito ao estudante: Welerson Cassamasso Barbe

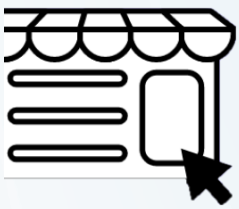
DICAS PARA COMPRAR ON-LINE

Compre de sites confiáveis

Lojas famosas ou franquias conhecidas sempre possuem um ótimo serviço de vendas online.

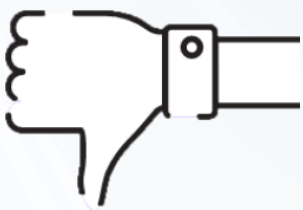
Busque pela avaliação da loja onde você compra

Existem diversos sites que as pessoas avaliam como foi sua experiência com alguma loja como a Reclame aqui.



Desconfie de preços muito absurdos

Preços muito baratos ou muito caros podem ser algum tipo de golpe, sempre desconfie disso quando for fazer suas compras.



Não compre nada por meio de redes públicas

Redes públicas são uma porta gigantesca e dados pessoais.
Sempre procure mexer com informações sensíveis em redes privadas.

Crédito ao estudante: Leonardo Bratfisch Sevalhos

SEGURANÇA DA INFORMAÇÃO PARA TODOS

CARTILHA GERADA A PARTIR DAS PUBLICAÇÕES REALIZADAS PELOS ALUNOS DO PROJETO DE EXTENSÃO SEGURANÇA DA INFORMAÇÃO PARA TODOS DA UNISAGRADO, DURANTE O ANO DE 2021.

UNISAGRADO
Ensino Superior de Excelência