



Margarida Duarte

Cibersegurança nas Escolas 2022

Para assinalar “O mês da Cibersegurança nas Escolas 2022”, os alunos da escola básica professor João Cónim pesquisaram e sugeriram algumas dicas sobre os temas Phishing e Ransomware.

Turma 9ºAE

N°2 e N°6

1

Automatic Zoom

Nº9 nº17



Phishing

É uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito.

São comunicações falsificadas praticada por criminosos chamados phishers que parecem vir de uma fonte confiável.

Como podemos evitar:

- Evitar clicar em links incorporados em e-mails,
- Seja cauteloso ao receber mensagens de fornecedores ou terceiros;
- Ativar a dupla verificação para ter mais segurança.



Ransomware

É um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate.

Dicas para evitar se tornar uma vítima de ransomware:

- Desconfiar de anexos e links enviados por e-mails, aplicativos e redes sociais.
- Verificar sempre quem é o remetente da mensagem.
- Evitar clicar ou abrir arquivos que não estejam sendo esperados.



Nº 7

5 / 36

Nº12

1 of 1 Automatic Zoom

CIBERSEGURANÇA NAS ESCOLAS 2022



PHISHING- É UM DOS MAIS ANTIGOS GOLPES DA INTERNET, PODEMOS DEFINIR PHISHING COMO QUALQUER TIPO DE FRAUDE POR MEIOS DE TELECOMUNICAÇÃO

RANSOMWARE- É UM DOS MAIS PROVÁVEL DE SER DETECTADO POR UM SOFTWARE DE SEGURANÇA. OBVIAMENTE, ALTERAÇÕES NAS EXTENSÕES DE ARQUIVOS



- - EVITE INSTALAR SOFTWARES SUSPEITOS A QUANTIDADE DE PLUG-INS MALICIOSOS TEM CRESCIDO COM O TEMPO.
- -EVITE SER AMIGÁVEL DEMAIS NAS REDES SOCIA.

Phishing e Ransomware

Nº18

Phishing Ransomware

CiberSegurança
NAS ESCOLAS



Ransomware é um código malicioso que impede que os utilizadores acessem aos seus arquivos ou sistemas. Estes são liberados somente, após o pagamento de resgate aos criminosos cibernéticos responsáveis.

Phishing é uma prática que os cibercriminosos tentam cometer enganando suas vítimas, ligando ou enviando uma mensagem (via e-mail, SMS, Whatsapp, etc.) para que a vítima baixe um arquivo infectado ou visite um site falso, obtendo dados confidenciais, bancos, senhas entre outros.

Ransomware



VS

Malware



VS

Phishing



Dica 1

Nunca clique em links ou anexos de e-mail constatavéis.

Dica 2

Evite divulgar informações pessoais.

Dica 3

Mantenha os seus sistemas operacionais e programas atualizados.

Web site: [Padlet.com](https://www.Padlet.com)

7 / 36

Phishing e Ransomware

Nº4



PHISHING E RANSOMWARE



PHISHING

É um tipo de fraude utilizado por meios de telecomunicação, que utiliza estratégias e psicológicas para manipular comportamentos e obter dados privados da vítima. Para a vítima voltar a reaver os seus dados terá de pagar uma quantia em dinheiro.

RANSOMWARE

O Ransomware é um tipo de malware que impede os utilizadores de aceder ao seu sistema ou até ficheiros pessoais e impõe o pagamento de um resgate para que o utilizador possa repor o acesso. Os golpistas do ransomware exigem o pagamento através de criptomoeda ou cartão de crédito.



como evitar:

- Navege online com segurança
- Use apenas redes seguras
- Leve a proteção de senhas a sério

Nº1 e Nº15

CiberSegurança



NAS ESCOLAS

Phishing e Ransomware

Phishing- É uma tentativa de fraude online, utilizada por criminosos para obter ilegalmente informações como o número da identidade, senhas bancárias, número do cartão de crédito, entre outras.



Ransomware- É um tipo de ataque virtual no qual um computador, quando infectado, os seus dados encriptados são impossíveis de acessar.



Dicas:

- 1- Não forneça informações pessoais.
- 2- Nunca clique em links de e-mails desconhecidos.
- 3- Não abra anexos de e-mails suspeitos.

Made with PosterMyWall.com

9 / 36

Phishing e Ransomware

Nº13

1 of 1 Automatic Zoom

RANSOMWARE E PHISHING

CiberSegurança



A RANSOMWARE É UM TIPO DE MALWARE QUE ROUBA OS DADOS DE UMA PESSOA E PARA VOLTAR A REAVÊ-LOS PRECISAMOS DE PAGAR UMA ALTA QUANTIA DE DINHEIRO.



O PHISHING É UMA TÉCNICA, UTILIZADA PARA ENGANAR PESSOAS NA INTERNET, COM OBJETIVO DE CONSEGUIR ROUBAR INFORMAÇÕES PESSOAIS DE UMA PESSOA OU EMPRESA.



COMO PREVENIR?

- NÃO DEVEMOS INSTALAR APLICAÇÕES DE TERCEIROS DA INTERNET.
- TER O ANTIVÍRUS E O SISTEMA OPERATIVO ATUALIZADO.
- DESCONFIAR DOS E-MAILS QUE PESSOAS DESCONHECIDAS ENVIAM.
- NÃO COLOCAR O CARTÃO DE CRÉDITO OU INFORMAÇÕES PESSOAIS EM SITES DESCONHECIDOS.

nº3 nº10

Nº3 E Nº10

Phishing e Ramsoware

Phishing

É tecnica que é usada para roubar informações pessoais pela internet normalmente feita por emais.

Ransomware

É um tipo de malware que bloquela o utilizador de aceder ao seu sistema ou ficheiros e pede dinheiro em troca de devolver o acesso.

Como evitar:

- Nunca cliques em links inseguros.
- Evite a divulgação de informações pessoais.
- Não abra anexos de e-mail suspeitos.
- Manter o sistema atualizado.
- Mantenha o antiviros e firewall atualizados.
- Não cliques em links suspeitos.

CiberSegurança



nº11



CIBERSEGURANÇA NAS ESCOLAS

Outubro 2022 - Mês da Cibersegurança

Phishing é um dos tipos mais conhecidos de cyber ataque. Consiste em enganar pessoas para obter informações pessoais.

A maneira mais usada para fazer este tipo de cyber ataque é se fazer passar por empresas para adquirir dados de cartões de crédito ou outros.





Ransomware é um software malicioso que encripta, ou fecha, ficheiros no computador que foi infetado, não permitindo que o utilizador tenha acesso aos mesmos.

As pessoas que bloqueiam estes ficheiros normalmente pedem transferências de dinheiro.

Também podem pedir moedas digitais como Bitcoin, Ethereum ou outros.

Como se proteger destes ataques

- Deve-se sempre verificar se o sítio de onde está a pagar, comprar ou fazer download de alguma coisa é confiável.
- Mudar frequentemente a sua password
- Ter sempre um antivírus ativo no seu computador

Nº5 e Nº14

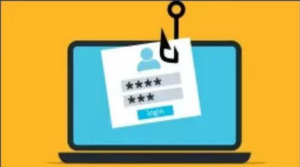
PHISHING E RANSOMWARE

Phishing

O Phishing é um crime que engana as pessoas, levando-as a partilhar informações pessoais, tais como palavra-passe, número de telemóvel e cartão de crédito.

Dicas para evitar o phishing:

- Verificar os links
- Confira a origem das mensagens
- Não forneça informações pessoais



Ransomware

É um tipo de malware (software malicioso) que impede os utilizadores de aceder aos seus ficheiros pessoais e exige-lhes o pagamento para devolver o acesso.

Dicas para evitar o Ransomware

- Fazer backup de dados
- Evitar divulgar dados pessoais
- Fazer download apenas de sites confiáveis



© 2019 - All Rights Reserved by Padlet.com



Turma 9ºBE

Nº20 Nº13

n°8 e n°21



Escola Básica Professor João Cónim

PHISHING

- 1- evitar clicar em links incorporados em e-mails
- 2- Proteja seus dados
- 3- Mantenha programas antivírus atualizados

O ATAQUE É REALIZADO POR MEIO DE COMUNICAÇÕES ELETRÔNICAS, COMO E-MAIL OU POR TELEFONE.



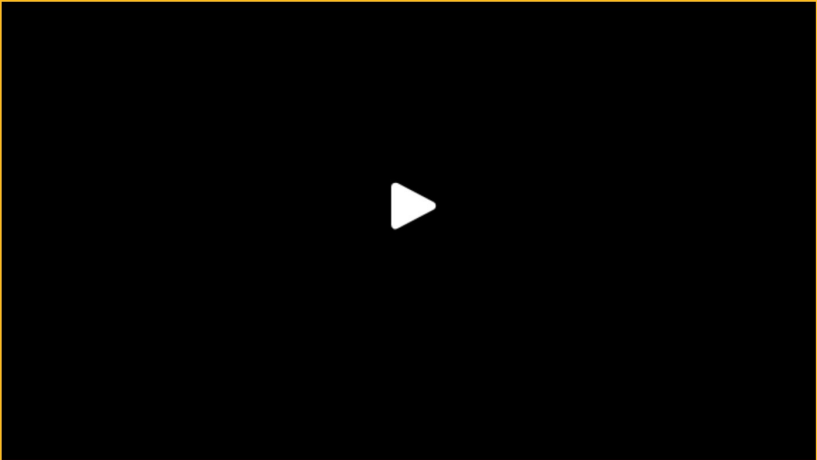
Ransomware

- 1- FAÇA BACKUP DE SEUS DADOS
- 2- NAVEGUE ON-LINE COM SEGURANÇA
- 3- USE APENAS REDES SEGURAS

O RANSOMWARE REPRESENTA UMA AMEAÇA PARA VOCÊ E SEU DISPOSITIVO



N°12 E N°17



Phishing e Ransomware

Nº3 e Nº15

Maneiras de prevenção

É importante manter o seu sistema atualizado com antivírus e desconfie de todos os e-mails que receber.

Phishing

É uma técnica usada para enganar usuários de internet, usando a fraude para obter informação confidenciais, por exemplo senha de cartões de crédito e nomes de usuários.

Ransomware

Deve de investir num software de cibersegurança; procurar por funções que irão proteger os programas vulneráveis contra as ameaças; tem que fazer cópias de segurança dos seus dados...

É um vírus que impede os utilizadores de aceder aos seus ficheiros pessoais ou ao seu sistema exigindo-lhes o pagamento de um resgate para devolver o acesso.



Nº18

1 of 1 Automatic Zoom

CiberSegurança

NAS ESCOLAS

PHISHING



- Phishing é o crime/fraude eletrônica mais simples e mais utilizada de ciberataque e, ao mesmo tempo é a mais perigosa e eficaz da atualidade.
- Phishing é o crime que engana as pessoas, levando-as a partilhar dados pessoais, como palavras-passe e números de cartões de crédito entre outros dados pessoais.

Dicas para proteger do Phishing:

- Nunca abrir as ligações de emails suspeitos de pessoas que não conhecemos;
- Quando receber esse email denunciá-lo e eliminá-lo;
- Utilizar antivírus.

RANSOMWARE



- Ransomware é um tipo de malware que impede os utilizadores de aceder ao seu sistema ou ficheiros pessoais fazendo com que depois seja exigido um resgate monetário para desbloqueá-lo.
- Malware abrange todo software malicioso que pode ser perigoso para o seu computador, incluindo vírus.

Dicas para proteger do Ransomware:

- Manter software sempre atualizado;
- Utilizar equipamentos adequados de backup;
- Ter cuidado com a navegação na internet.

Nº4 e 11

1 of 1 Automatic Zoom

CiberSegurança

PHISHING E RANSOMWARE

Segurança NAS ESCOLAS

Phishing

É UMA TÉCNICA DE CRIME CIBERNÉTICO QUE USA FRAUDE, TRUQUE OU ENGANO PARA MANIPULAR AS PESSOAS E OBTER INFORMAÇÕES CONFIDENCIAIS.



Ransomwere

É UM TIPO DE MALWARE QUE BLOQUEIA O ACESSO A ARQUIVOS OU SISTEMAS, SENDO DEPOIS COBRADO UM VALOR PELO RESGATE DOS DADOS, O QUE TORNA QUASE IMPOSSÍVEL RASTREAR O CRIMINOSO.



PROTEJA-SE

22 / 36

Turma 9ºCE

nº8

CIBERSEGURA NAS ESCOLAS

Outubro 2022 - Mês da Cibersegurança

- Instale antivírus
- Nunca clique em ligações ou anexos em e-mails suspeitos.
- Se a mensagem suspeita parecer ser proveniente de uma pessoa que conhece, contacte essa pessoa através de outros meios, por exemplo, mensagem de texto ou chamada telefónica para confirmar.

Phishing

Ransomware

1. Nunca clique em links inseguros.
2. Evite a divulgação de informações pessoais.
3. Não abra anexos de e-mail suspeitos

24 / 36

nº13



CiberSegurança



NAS ESCOLAS

Phishing

- Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.
- Os responsáveis pelo phishing criam mensagens falsas que incorporam cores, logotipos, slogans e outras características da identidade de alguma instituição conhecida. O motivo é óbvio: fazer o usuário acreditar que aquela entidade está se comunicando com ele.

Ransomware

Ransomware é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

O resgate é cobrado em criptomoedas, que, na prática, o torna quase impossível de se rastrear o criminoso.



25 / 36

nº2

1 of 1Automatic Zoom



CiberSegurança

SeguraNet: NAS ESCOLAS

Phishing

é uma **técnica de fraude online**, utilizada por criminosos no mundo da informática para **roubar senhas de banco e demais informações pessoais**, usando-as de maneira fraudulenta.



nº3

1 of 5

Automatic Zoom

CiberSegurança

NAS ESCOLAS

Phishing e Ransomware



O que é o Phishing?

▶ Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais. Saiba como ele funciona para poder detectar e bloquear golpes de phishing e manter seus dados protegidos contra invasores. Proteja-se contra ataques de phishing com o Avast Free Antivirus.



Como evitar o Phishing ?

- ▶ saber que ele existe
- ▶ Cuidado na utilização da internet
- ▶ Altere imediatamente as palavras-passe

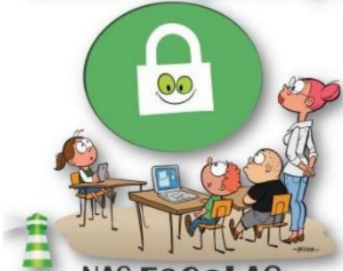
27 / 36

1 of 2 Automatic Zoom

Phishing? O que será?

É uma maneira de roubar dados de outras pessoas

CiberSegurança



SeguraNet NAS ESCOLAS

Como podemos evitar:

- Não aceder a sites desconhecidos porque podem não ser seguros.
- Não dar os nossos dados a ninguém.



Ransomware

Roubo de dados que usa como refém arquivo das pessoas para depois pedir dinheiro. para restabelecer o acesso a estes arquivos O resgate é

Phishing

nº15 nº17

1 of 2

Automatic Zoom

Phishing

Phishing é uma técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

Como evitar

- 1- DESCONFIE DE TODOS OS E-MAILS QUE RECEBER
- 2- MANTENHA SEU SISTEMA ATUALIZADO
- 3- MANTENHA ANTIVÍRUS E FIREWALL ATUALIZADOS



ransomware

- O ransomware representa uma ameaça para você e seu dispositivo, mas o que torna essa forma de malware tão especial? Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.
- Como evitar:
- Nunca clique em links inseguros.
- Evite a divulgação de informações pessoais.
- Use apenas fontes de download conhecidas.



Phising

nº14

1 of 2

Automatic Zoom

Como nos prevenir do Phishing?

- Não abrir emails de remetentes que não sejam conhecidos familiares.
- Nunca clicar num link num email, a menos que saiba exatamente onde irá ter.
- Se suspeitar de que um email não é fidedigno, insira um nome ou um texto da mensagem num motor de busca para ver se existe algum ataque de phishing conhecido que recorra aos mesmos métodos.

O que é o Phishing?

PHISHING É O CRIME DE LUDIBRIAR AS PESSOAS, LEVANDO-AS A PARTILHAR INFORMAÇÕES CONFIDENCIAIS, COMO PALAVRAS-PASSE E NÚMEROS DE CARTÕES DE CRÉDITO.

O que é o Ransomware?

- Ransomware é um tipo de malware que criptografa arquivos e até sistemas de computador inteiros e, em seguida, exige o pagamento de um resgate para devolver o acesso.

Como nos prevenir do Ransomware?

- Use um bloqueador de anúncios.
- Faça backup regularmente do seu sistema.
- Mantenha seus softwares atualizados.



30 / 36

Nº4 & Nº10

1 of 2

Automatic Zoom

PHISHING

O QUE É?

Phishing é o crime de ludibriar as pessoas, levando-as a partilhar informações confidenciais, como palavras-passe e números de cartões de crédito.

Tal como na pesca ("fishing", em inglês), há mais de uma forma de apanhar uma vítima, mas há uma tática de phishing que é mais comum.

As vítimas recebem um email ou uma mensagem de texto que imita uma pessoa ou organização em que elas confiam, como um colega, o banco ou uma entidade governamental

Como prevenir?

- Desconfiar de todos os e-mails que se receber.
- Manter o sistema do computador/telemóvel/tablet atualizado.
- Manter o antivírus e firewall atualizados.
- Utilizar o padrão DMARC.



Nº4 & Nº10

Ransomware

O QUE É?

O ransomware é um tipo de Badware de rapto de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra o resgate para reestabelecer o acesso a estes arquivos.

COMO EVITAR?

Primeiramente fazer Backups regulares do sistema.

Treinar os funcionários para evitar Phishing e outro tipo de golpes.

Exigir o uso de uma plataforma ENTERPRISE Password Management (EPM), como o Keeper.



31 / 36

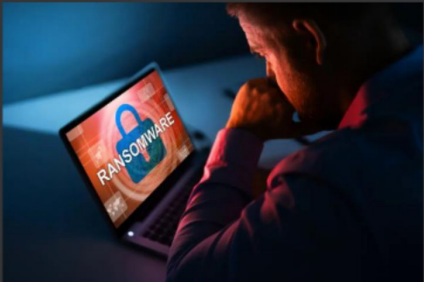
32 / 36

1 of 4

Automatic Zoom

Agrupamento escolas Rio Arade

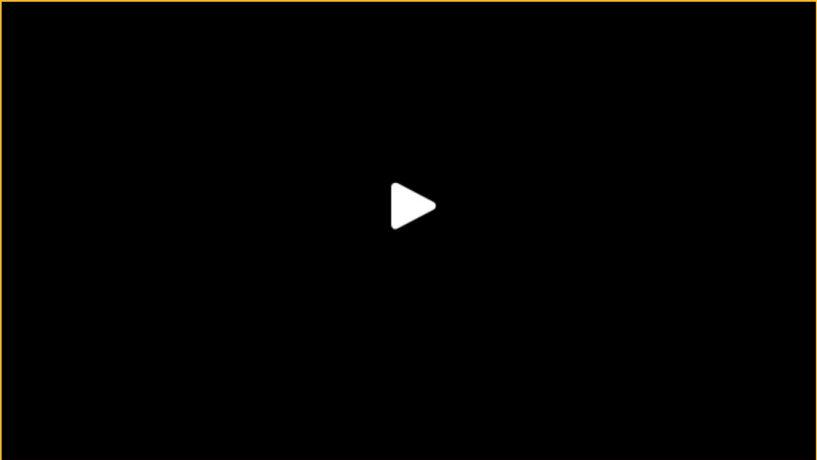
Phishing e Ransomware



Cibersegurança

A Cibersegurança tem a ver com a proteção de...

n°9



nº 7 e nº11

1 of 5

Automatic Zoom

Phishing e Ransomware

O que é Phishing?

Phishing trata-se de roubo de identidades online, ou seja, tentativa de adquirir dados pessoais de outra pessoa, como por exemplo:

- Dados financeiros
- Senhas pessoais
- Número de cartões de crédito

• O golpista usa aplicativos, sites e emails que servem especificamente para roubar dados pessoais. Se fazem passar por pessoas/empresas confiáveis, desta maneira, depois de mandar a mensagem apenas aguardam que a vítima

Como fazem

Phishing

Nº16

1 of 1

Automatic Zoom

Phishing

CiberSegurança



NAS ESCOLAS

O phishing é qualquer tentativa de adquirir a informação pessoal de outra pessoa, ou outros detalhes pessoais, por meios ilícitos. O phishing envolve normalmente e-mails fraudulentos ou websites que tentam enganar potenciais vítimas e levá-las a partilhar informação sensível com o malfeitor por detrás da fraude.

• Como evitar o phishing:

- Avaliar sempre a oportunidade dos conteúdos de *emails*, de mensagens instantâneas, de SMS ou de telefonemas;
- Não partilhar dados sensíveis nas redes sociais porque essa prática pode fornecer informação a possíveis atacantes que queiram realizar *spear phishing* (phishing dirigido a uma pessoa específica)

