DELL Technologies

Documento de referência para a segurança cibernética

Em um mundo cada vez mais virtual, não é de se surpreender que o crime cibernético esteja crescendo a uma velocidade assustadora. Na verdade, **o crime cibernético gerou cerca de US$ 6 trilhões em 2021**, o que o tornou a terceira maior economia do mundo, atrás dos EUA e da China![1] Os invasores têm ficado cada vez mais espertos e aprimorados, mas é fácil manter a segurança on-line quando conhecemos as ameaças mais recentes e implementamos medidas de proteção. **Estas são algumas das ameaças nas quais os especialistas em segurança cibernética da Dell estão trabalhando para tentar evitá-las. Também temos dicas de como manter a segurança em casa e no local de trabalho.**

Compromisso a ser seguido

Pessoas mal-intencionadas têm acesso ao sistema quando você cai em um site desprotegido ou que apresenta riscos.

Como detectar:

Arquivos novos ou conexões de rede que você não adicionou ao sistema

Pedidos indesejados de informações de configuração

DICA: *Mantenha os navegadores e plug-ins atualizados*

A sua conexão não é segura.

Hardware desprotegido

DICA: *Faça compras com vendedores autorizados*

Sabia que a impressora também pode ser hackeada?

Agentes de ameaça adicionam vulnerabilidades diretamente aos hardwares e acessórios.

Como detectar:

Descontos bons demais para serem verdadeiros

Engenharia social

O impostor manipula as pessoas fingindo ser uma pessoa jurídica ou outro órgão oficial para roubar as **informações pessoais ou financeiras confidenciais delas** (prática também conhecida como "phishing"). O código mal-intencionado é enviado por links ou anexos aos e-mails, mensagens diretas ou textos.

Como detectar:

E-mails ou mensagens indesejadas que pedem informações pessoais com instruções para abrir links e anexos

Endereço de e-mail, texto e ortografia do remetente que causam estranheza

DICA: *Órgãos governamentais (serviço de receita etc.) entrarão em contato por correio inicialmente*

Algo suspeito por aqui?

Ataque de malware via pen drive

DICA: *Tenha cuidado com pen drives desconhecidos, mesmo que tenham sido compartilhados entre amigos*

Hmm... Será que é seguro conectar esta pen drive?

O hacker usa dispositivos de armazenamento removível, como pen drives, HDs externos, smartphones, tocadores de música, cartões SD e discos de mídia óptica (CDs, DVDs e Blu-ray), para contaminar um computador ou rede.

Como detectar:

Acesso inesperado aos documentos ou arquivos recém-criados no dispositivo

Relacionamento de confiança

O hacker viola outro local de confiança, como o consultório de um médico, e usa a reputação dele para explorar os pacientes.

Como detectar:

Comportamento estranho ao fazer log-in

DICA: *Use senhas difíceis e únicas*

Quem é você?

Como manter a segurança cibernética:

O QUE FAZER

Use a autenticação baseada em vários fatores, bem como senhas difíceis e únicas em todas as contas.

Qualquer dispositivo conectado à Internet está sujeito a ataques. Mantenha os softwares atualizados.

Mantenha-se alerta e desconfie sempre. Aprenda a reconhecer as táticas dos impostores.

Fale do que aconteceu. Denuncie os ataques à equipe de TI e avise colegas, parentes e amigos.

O QUE NÃO FAZER

Não durma no ponto. Siga todos os protocolos de segurança sempre.

Não clique em nenhum link adicionado a e-mails indesejados ou mensagens diretas.

Não ignore mensagens do navegador, como "A sua conexão não é segura" ou "A sua conexão não é privada".

DICA: *Para obter mais informações, acesse:* Dell.com/Endpoint-Security

DELL Technologies

[1]Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics