SECURITY HINTS & TIPS

Unsafe Email Attachments

Many people use email in their personal life and their workplace. You can get an email from your aunt with her stew recipe or an email from your boss with a guest list for the office party. But what if the email isn't actually from your aunt or boss? Cybercriminals often pretend to be someone you know to get you to click unsafe attachments, such as fake DOC files or PDF files. Some of the most common attachments used for attacks are DOC files and PDF files. It's important to learn how to identify unsafe email attachments and protect yourself.

Fake DOC Attachments

Older Microsoft Word DOC files are commonly used in cyberattacks because they can include macros. A macro, short for macroinstruction, is a set of commands that can control a DOC file and other programs. Cybercriminals may send you an email with a DOC file that contains a macro. The email usually looks legitimate and gives an urgent reason for you to open the file. If you open the file, a pop-up window will display asking you to enable macros. If you accept, the macros will be able to install malware on your device.

Fake PDF Attachments

PDF files are sent over email every day, making them perfect tools for cyberattacks. One popular type of attack is when cybercriminals put an image in a PDF file to trick you into clicking it. For example, it could be an image that looks like a video with a play button. The image will be something that catches your attention, like a cooking video from social media or a cute cat video. Unfortunately, clicking the image could send you to a website designed to steal your sensitive information.

What Can I Do to Stay Safe?

Follow the steps below to stay safe from dangerous email attachments:

- If a suspicious email appears to be from someone you know, contact them over the phone or in person. Check to see if the email is legitimate before putting yourself at risk.
- Avoid DOC files in general. They use an outdated format and contain too many security risks. The newer DOCX format is the current standard and is much safer.
- Always think before you click. Cyberattacks are designed to catch you off guard and trick you into clicking impulsively.

Erb

KnowBe4
Human error. Conquered.

SECURITY HINTS & TIPS

Social Media

Social media and all its greatness is an excellent way to catch up with old colleagues, friends, and family. It's also fabulous to see all the pictures of people's wonderful trips, what people had to eat, family photos and all sorts of celebrations. Although, with all great things on the internet, there are also ways for bad guys to get information out of you, and now more than ever, you must be very cautious of the scams and hackers out there.

Clicking on Links

Whether it's to install a new money-making stock trading app or a job you can work from home in your spare time, you need to click on the link to install the app. BAM! Next thing you know, they have full control of your phone and everything you have stored on there.

Always be mindful of anything you post online, as it may harm you in the future. A job interview or information hinting your password at work or any site you may visit.

AI Chatbots

AI Chatbots are a great way to get all sorts of information, but with all great information comes greater responsibility! As easy as it is to get information from the chatbots, it's also easy to get information from you. With its intelligence, AI can look for key phrases anywhere on the internet to generate more convincing and sophisticated fake news, propaganda and other malicious content.

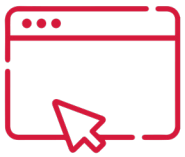
Deepfakes are a Real Threat

Protect yourself and your organization from deepfakes.

A deepfake is described as a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information

Be sure to evaluate any suspicious audio or video. Visual flaws can indicate whether or not the video or audio is real.

Pay attention to your emotions. It's important to stop, look, and think before you take any type of action.



Leverage deep fake detection software that is available and always remain alert and cautious.

If you notice anything suspicious, please report it immediately.

KnowBe4
Human error. Conquered.

SECURITY HINTS & TIPS

Be Fearful and Aware!

Every 39 seconds, someone is hit with a malicious cyber-attack. The bad guys will target everyone, not just big companies. They want your money; if you want to keep it, be suspicious and mindful. Always double-check emails and texts for incorrect spelling, grammar mistakes, anything wanting you to act fast, hyperlinks and the time of day the email and text are sent. The bad guys are out there, and we need our champions to help us keep ourselves and our company safe.

Ransomware is one of the worst forms of cyber-attacks. With one click, you've let the attackers in, and now they can encrypt all files on your computer and network. Unfortunately, the only way to unlock the files is to pay them a huge sum, which will not even guarantee getting the files back.

Knowledge is Key - Prevent Ransomware attacks with these tips

1. **Checking the domain of the email sent is a key sign, but you should also be aware of the username.**
   - username@erbgroup.com – Good
   - username@erbgroup-mail.com – Bad
   - username@erb.group.com – Bad
2. **Check to see if the email subject is looking for an instant response.**
   - Hurry now and sign-up
   - Urgently
3. **Don't click any links.**
4. **Follow up with the sender.**
   - If you receive an email from IT or someone from a company needing money or sending file share you are unaware of, call them to verify the email's authenticity.
5. **Check spelling and grammar mistakes.**

PUMP UP

YOUR PASSWORD STRENGTH

Cybercriminals love weak passwords! **Protect yourself and your organization** with these best practices.

Make passwords **hard to guess**

Use a different password for each app and website

Change your password regularly

Don't share your password

KnowBe4
Human error. Conquered.

ASTUCES DE CYBERSÉCURITÉ

Pièces jointes malveillantes

De nos jours, tout le monde utilise le courriel au travail et à la maison. Que ce soit un courriel de votre tante qui partage avec vous sa nouvelle recette de ragoût ou un courriel de votre patron qui vous annonce la liste des invités à la fête de bureau, on utilise tous le courriel. Toutefois, c'est possible que le courriel que vous recevez ne soit même pas de la part de votre tante ou de votre patron. En fait, les cybercriminels se font souvent passer pour quelqu'un que vous connaissez afin de vous inciter à cliquer sur une pièce jointe malveillante telle qu'un fichier DOC ou PDF piégé. Certains des fichiers les plus utilisés pour des cyberattaques sont en fait des fichiers DOC et PDF. Il est important pour vous d'apprendre à identifier une pièce jointe malveillante pour vous protéger des cybercriminels.

Fichiers DOC piégés

Les anciennes versions du fichier DOC de Microsoft Word sont souvent utilisées à des fins de cyberattaques parce qu'elles contiennent des macros. Une macro, forme abrégée de « macro-instruction », constitue un ensemble de commandes qui contrôlent un fichier DOC ainsi que d'autres logiciels. Il est possible qu'un cybercriminel vous envoie un courriel avec une pièce jointe qui contient une macro. Le plus souvent, un tel courriel a l'air légitime, mais il affiche une raison urgente qui vous incite à ouvrir le fichier sans tarder. Si vous l'ouvrez, une fenêtre apparaît qui vous demande d'activer les macros. Et si vous les activez, elles installent des logiciels malveillants sur votre ordinateur.

Fichiers PDF piégés

Chaque jour, on envoie de nombreux fichiers PDF par courriel, raison pour laquelle ils constituent le fichier de premier choix des cybercriminels. Une cyberattaque commune consiste à mettre une image dans un PDF qui vous incite à cliquer dessus. Par exemple, il peut s'agir d'une image qui ressemble au bouton « lecture ». Cette image attire votre attention, comme une vidéo de recettes sur les réseaux sociaux ou une vidéo d'un chat mignon. Malheureusement, si vous cliquez sur cette image, elle peut vous diriger vers un site Web qui vous vole vos renseignements sensibles.

Comment puis-je me protéger des pièces jointes malveillantes?

Pour vous protéger des pièces jointes malveillantes, vous devez suivre les étapes suivantes :

- Si vous recevez un courriel suspect de la part de quelqu'un que vous connaissez, contactez cette personne par téléphone ou parlez-lui en personne pour savoir si c'est véritablement elle qui vous l'a envoyé. Il est important de vérifier si le courriel est légitime avant de vous exposer à un tel risque.
- De manière générale, il vaut mieux éviter les fichiers DOC. Il s'agit d'un format obsolète qui présente trop de risques à la sécurité en ligne. Le format DOCX, qui est plus récent, est un format plus sécurisé.
- Pensez toujours avant de cliquer. Une cyberattaque est conçue pour vous tromper quand votre garde est baissée et elle vous incite à cliquer sur un lien sans réfléchir.

Erb

KnowBe4
Human error. Conquered.

ASTUCES DE CYBERSÉCURITÉ

Les médias sociaux

Les médias sociaux et tout ça' grandeur, excellent moyen de rattraper le vieux collègue, les amis et la famille. C'est aussi fabuleux de voir toute l'image des gens de merveilleux voyages, ce que les gens devaient manger, des photos de famille et toutes sortes de célébrations. Bien que, avec toutes les grandes choses sur Internet, il y a aussi des moyens pour les méchants d'obtenir des informations de vous et maintenant plus alors jamais d'être très prudent de l'escroquerie et pirater là-bas.

En cliquant sur les liens

En cliquant sur les liens, que ce soit pour installer cette nouvelle application de trading d'actions rentable ou un travail que vous pouvez travailler à domicile pendant votre temps libre, il suffit de cliquer sur le lien pour installer l'application. BAM ! Ensuite, vous savez qu'ils ont le contrôle total de votre téléphone et de tout ce que vous y avez stocké.

Soyez toujours conscient

Soyez toujours conscient de tout ce que vous publiez en ligne car cela pourrait vous nuire à l'avenir. Un entretien d'embauche ou simplement des informations et un indice sur ce que votre mot de passe pourrait être au travail ou tout site que vous pouvez visiter.

Ai Chatbots

Ai Chatbots est un excellent moyen d'obtenir toutes sortes d'informations, mais avec toutes les grandes informations vient une plus grande responsabilité ! Aussi facile qu'il soit d'obtenir des informations des chatbots, il est également facile d'obtenir des informations de votre part. L'IA avec l'intelligence peut rechercher des phrases clés n'importe où sur Internet pour générer des faux nouveaux, de la propagande et d'autres contenus malveillants plus convaincants et sophistiqués.

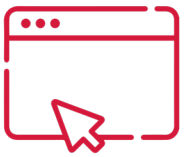
Les hypertrucages représentent une réelle menace.

Vous devez vous protéger et protéger votre entreprise des hypertrucages.

Une vidéo hypertruquée est une vidéo d'une personne dont le visage ou le corps a été altéré à l'aide de techniques de l'intelligence artificielle, de manière à ce qu'elle apparaisse comme quelqu'un d'autre. L'hypertrucage est souvent utilisé à des fins malveillantes ou pour diffuser de la désinformation.

Assurez-vous d'analyser un fichier audio ou vidéo suspect. Les erreurs visuelles peuvent indiquer si le contenu audio ou vidéo est falsifié ou non.

Écoutez vos émotions. Il est important de prendre un instant pour réfléchir avant de prendre quelque mesure que ce soit.



Faites appel aux logiciels de détection des hypertrucages et soyez prudents.

Si vous remarquez quelque chose de suspect, signalez la situation immédiatement.

KnowBe4
Human error. Conquered.

ASTUCES DE CYBERSÉCURITÉ

Soyez craintif et conscients !

Toutes les 39 secondes, quelqu'un est frappé par une cyberattaque malveillante, les méchants cibleront tout le monde, pas seulement les grandes entreprises. Ils veulent votre argent et si vous voulez le garder, soyez suspects et attentifs. Vérifiez toujours les e-mails et le texte incorrects, les fautes de grammaire, le désir que vous agissiez rapidement, les hyperliens et l'heure de la journée, les e-mails et le texte sont envoyés. Les méchants sont là-bas, et nous avons besoin de nos champions pour nous aider à assurer votre sécurité et celle de la compagnie.

Les ransomwares sont l'une des pires formes de cyberattaques, en un clic, vous avez laissé entrer les attaquants, et maintenant ils ont la capacité et crypteront tous les fichiers sur votre ordinateur et votre réseau. Malheureusement, la seule façon d'obtenir les fichiers déverrouiller est de leur payer une somme énorme et qui ne garantira même pas de récupérer les fichiers.

La connaissance est la clé - Prévenir les attaques de ransomware grâce à ces conseils

1. **Vérifier le domaine de l'e-mail envoyé est un signe clé, mais vous devez également connaître le nom d'utilisateur.**
   - username@erbgroup.com – Bon
   - username@erbgroup-mail.com – Mauvais
   - username@erb.group.com – Mauvais
2. **Vérifiez si l'objet de l'e-mail recherche une réponse instantanée.**
   - Dépêchez-vous maintenant et inscrivez-vous
   - D'urgence
3. **Ne cliquez sur aucun lien.**
4. **Faites un suivi auprès de l'expéditeur.**
   - Si vous recevez un e-mail de l'informatique ou quelqu'un de l'entreprise qui a besoin d'argent ou d'envoyer un partage de fichiers que vous ne connaissez pas, appelez-les pour vérifier l'authenticité de l'e-mail.
5. **Vérifiez les fautes d'orthographe et de grammaire**

Erb KnowBe4 Human error. Conquered.

RENFORCEZ

VOTRE MOT DE PASSE

Les cybercriminels adorent les mots de passe faibles. C'est pourquoi il est important de vous protéger et de protéger votre entreprise à l'aide de ces pratiques exemplaires pour choisir un mot de passe fort.

Créez un mot **de passe qui est difficile** à deviner

Utilisez un mot de passe **différent pour chaque application** ou site Web

Modifiez votre mot de passe de temps en temps

Ne divulguez jamais votre mot **de passe à qui que ce soit**