NEVER GET BEAT BY A BREACH!
SAFETY & SECURITY NEWSLETTER - JANUARY 2024

No one logs in to work for the day thinking, "Today is the day I will be compromised by a cybersecurity attack." And while you may not encounter a cyberthreat this month or even year, it is critical to stay alert to the trends and best practices. This month's newsletter will share a few of the important (but perhaps not so obvious) cybersecurity best practices to keep you and your organization safe this year.

CHECK EMAIL RECIPIENTS
Sending emails to the wrong people increases the chance of sensitive company or personal information being used by unauthorized individuals.

All information, especially sensitive information, should only be shared with those who need to know. This includes email contents. It is easy to click a recipient that pops up in your email without truly knowing that you clicked the right person. Emails that end up in the wrong hands may be used for malicious purposes.

INVESTIGATE HYPERLINK'S DESTINATION BEFORE CLICKING
Many times, we encounter websites in the form of hyperlinks. For example, a link that says, "Policy reminders" and takes you to a website or other destination. Hyperlink destinations can be viewed before clicking by hovering over the link with your mouse.

It is important to check the link's destination before clicking. Hackers know that users don't often check links before clicking, and they will hide malicious websites behind hyperlinks. Malicious websites can download malware, scam you or collect your credentials. By checking links, you can avoid these websites.

REVIEW YOUR ORGANIZATIONS SECURITY POLICIES AND PROCEDURES
Security policies are put in place to reduce the risk of cybersecurity incidents and increase awareness. In addition to staying up to date with the security policies, reviewing and following all cybersecurity procedures keeps cybersecurity best practices as a foundational part of your workday.

Shared from
INFOSEC

ARTISANS' BANK
www.ArtisansBank.com

FOLLOW US!