CYBERSECURITY AWARENESS MONTH

SEHEN SIE SICH SELBST IM CYBERSPACE (SEE YOURSELF IN CYBER)

Jeder spielt eine Rolle bei der Cybersicherheit... unabhängig von seiner Funktion.

Das Thema der Kampagne zum Monat der Cybersicherheit 2022 - "Sehen Sie sich selbst im Cyberspace" - zeigt, dass Cybersicherheit zwar ein komplexes Thema zu sein scheint, es aber letztlich um Menschen geht. Tragen Sie Ihren Teil dazu bei, sich selbst und die Cybersicherheit unseres Unternehmens zu schützen, indem Sie vier wichtige Punkte befolgen.

AKTIVIEREN SIE MULTI-FAKTOR-AUTHENTIFIZIERUNG

Multi-Faktor-Authentifizierung, auch als Zwei-Faktor-Authentifizierung und Zwei-Schritt-Verifizierung bekannt, ist eine Sicherheitsmaßnahme, die von jedem verlangt, der sich bei einem Konto anmeldet, seine Identität in einem zweistufigen Prozess zu beweisen. Dadurch wird es für Kriminelle doppelt so schwer, auf ein Online-Konto zuzugreifen. Durch das Hinzufügen eines einfachen Schrittes bei der Anmeldung bei einem Konto erhöht die Multi-Faktor-Authentifizierung die Sicherheit Ihres Kontos erheblich.

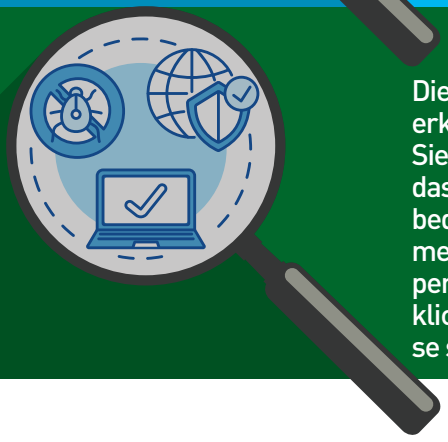
VERWENDEN SIE SICHERE PASSWÖRTER

Passwörter sind wichtig, wenn Sie Ihre Daten schützen wollen. Hier finden Sie einige einfache Möglichkeiten, Ihre Konten durch bessere Kennwortpraktiken zu schützen. Unabhängig von der Art des Kontos sollten Sie bei der Erstellung aller Passwörter diese drei Punkten beachten:

- Lang - Mindestens 12 Zeichen
- Einzigartig - Jedes Konto benötigt ein eigenes, einzigartiges Passwort
- Komplex - Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Bei einigen Websites können Sie sogar Leerzeichen einfügen.

AKTUALISIEREN SIE DIE SOFTWARE

Halten Sie Ihre Software immer auf dem neuesten Stand, wenn Updates verfügbar sind, und verschieben Sie das nicht. Diese Updates beheben allgemeine Softwareprobleme und bieten neue Sicherheitspatches für Bereiche, in die Kriminelle eindringen könnten. Wenn Sie ein Software-Update herunterladen, sollten Sie es nur von jenem Unternehmen beziehen, das es erstellt hat. Verwenden Sie niemals gehackte, raubkopierte oder nicht lizenzierte Software-Versionen, da diese oft Malware enthalten und mehr Probleme verursachen als lösen.



ERKENNEN UND MELDEN SIE PHISHING

Die Anzeichen können schwer zu erkennen sein, aber sobald Sie einen Phishing-Versuch erkennen, können Sie vermeiden, darauf hereinzufallen. Hier sind einige kurze Tipps, wie Sie eine gefälschte Phishing-E-Mail eindeutig ausmachen können: Enthält ein Angebot, das zu schön ist, um wahr zu sein; Formulierungen, die dringend, alarmierend oder bedrohlich klingen; schlecht formulierter Text mit Rechtschreib- und Grammatikfehlern; mehrdeutige oder sehr allgemein gehaltene Begrüßungen; Ersuchen um Übermittlung persönlicher Informationen; Drängen, auf einen unbekannten Hyperlink oder Anhang zu klicken; seltsame oder unerwartete geschäftliche Anfragen; die Absender-E-Mail-Adresse stimmt nicht mit dem Unternehmen überein, von dem die Nachricht stammt.

MAUSER
Packaging Solutions