# CYBERSECURITY AWARENESS MONTH

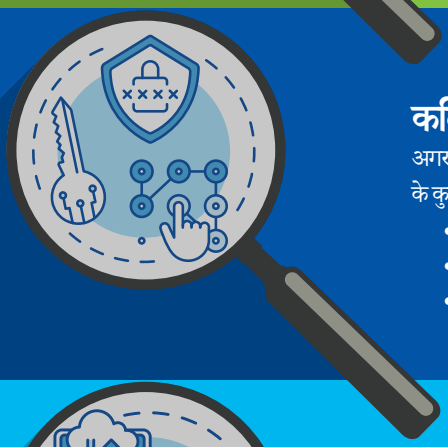
# खुद को साइबर में देखें
# (SEE YOURSELF IN CYBER)

*साइबर सुरक्षा में सभी लोग भूमिका निभाते हैं...इससे कोई फर्क नहीं पड़ता है कि आपकी भूमिका क्या है।*

2022 साइबर सुरक्षा जागरुकता माह के अभियान की थीम-"खुद को साइबर में देखें" —प्रदर्शित करती है कि हालांकि साइबर सुरक्षा एक जटिल विषय की तरह दिख सकता है, अंततः, यह पूरी तरह से लोगों के बारे में हैं। चार प्रमुख कार्यवाहियों का अनुसरण करके खुद की और हमारी कंपनी की साइबर सुरक्षा को सुरक्षित रखें।

## बहुकारकीय प्रमाणीकरण सक्षम करें

इसे दो-कारक प्रमाणीकरण और दो-चरण के प्रमाणीकरण के रूप में भी जाना जाता है, यह एक सुरक्षा तरीका है जिसकी जरूरत किसी को भी एक अकाउंट लॉगिन करने में अपनी पहचान को प्रमाणित करने के लिए दो-चरण की प्रक्रिया में नेवीगेट करने के लिए होती है। यह अपराधियों के लिए खाते में एक्सेस करने को दोगुना कठिन बना देता है। अपने अकाउंट में लॉगिन करते समय एक और साधारण चरण को शामिल करने से,बहु-कारकीय प्रमाणीकरण आपके खाते की सुरक्षा को बहुत अधिक बढ़ा देता है।



## कठिन पासवर्ड का प्रयोग करें

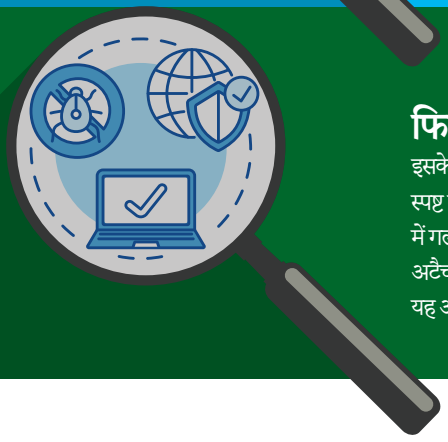
अगर आप अपनी जानकारी को सुरक्षित रखना चाहते हैं तो पासवर्ड महत्त्वपूर्ण हैं। यहां पर सर्वोत्तम पासवर्ड आदतों के जरिए आपके खाते को सुरक्षित करने के कुछ आसान तरीके दिए गए हैं। खाता कोई भी हो, सभी पासवर्ड इन तीन शब्दों को ध्यान में रखते हुए बनाए जाने चाहिए।

- लंबे–कम से कम 12 वर्ण के
- अद्वितीय- हर एक खाते को अपेन एक अद्वितीय पासवर्ड की जरूरत होती है
- जटिल-अपरकेस (कैपिटल) और लोअरकेस (स्मॉल) अक्षरों तथा विशेष अक्षरों के एक संयोजन का प्रयोग करें। कुछ वेबसाइटें आपको स्पेस को शामिल करने की अनुमति देती हैं।

## सॉफ्टवेयर को अपडेट करें

जब भी अपडेट उपलब्ध हो हमेशा अपने सॉफ्टवेयर को अपडेट करें और देर न करें।

ये अपडेट सामान्य सॉफ्टवेयर समस्याओं को ठीक कर देते हैं और नए सुरक्षा पैच प्रदान करते हैं जहां अपराधी प्रवेश कर सकते हैं। कोई सॉफ्टवेयर अपडेट डाउनलोड करते समय, केवल इसे उसी कंपनी से प्राप्त करें जिसने इसे बनाया हो। सॉफ्टवेयर के हैक किए गए, निजी या बिना लाइसेंस के संस्करण का प्रयोग कभी भी न करें क्योंकि अक्सर इनमें मालवेयर होते हैं और ये समाधान करने से अधिक समस्याएं उत्पन्न करते हैं।



## फिशिंग की पहचान करें और रिपोर्ट करें

इसके संकेत जटिल हो सकते हैं, लेकिन जब आप फिशिंग के प्रयासों को पहचान लेंगे तो आप इसमें पड़ने से बच सकते हैं। एक फेक फिशिंग ईमेल का स्पष्ट तौर पर कैसे पता लगाना है इसके लिए यहां पर कुछ त्वरित टिप्स दिए गए हैं: इसमें एक ऐसा ऑफर है जो अविश्वसनीय रूप से अच्छा है; स्पेलिंग में गलतियां, खराब गुणवत्ता का लेखन, और खराब व्याकरण है; व्यक्तिगत जानकारी भेजने का अनुरोध किया गया है; किसी अनजान हाइपरलिंक या अटैचमेंट पर क्लिक करने की जल्दबाजी है; विचित्र या आकस्मिक व्यवसाय अनुरोध ; भेजी गई ईमेल का पता उस कंपनी से मिलान नहीं खाता है जिससे यह आई है।

MAUSER
Packaging Solutions