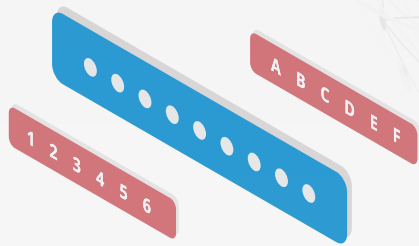




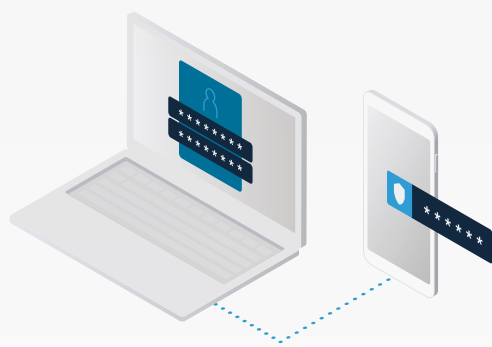
How You Can Fight Foreign Hackers

Don't let bad actors from Russia—or any other country—take advantage of you. Most cyber attacks start when an end user accidentally lets the bad guys into the system. But following these simple rules will help you defend your data at work and at home.



Choose a Strong Password

This simple step can prevent a lot of data breaches. The best passwords are abbreviations of phrases you can easily remember such as “WW2DN21!” (“We went to Disney in 2021”).



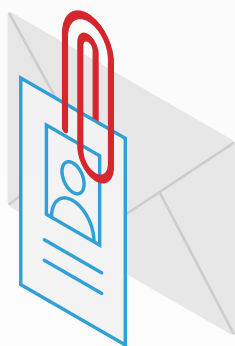
Use Multifactor Authentication (MFA) When It's Available

This is the feature that texts a code to your phone when you attempt to log into systems. Using MFA stops almost all breaches because foreign hackers have almost no chance of ever seeing your phone.



Think Before You Click

Closely check links in emails before you click them. The link may have a familiar name (like Microsoft or Amazon) but really point to a fraudulent address that steals information. Hover your mouse over a link to see where it's going to take you.



Don't Open Unexpected Files

Whether files come to you as an email attachment or even on a USB drive you find in the office, don't open anything you weren't expecting to receive. Be cautious even if the files seem to come from a user you know. Hackers can impersonate known users via email.



Check Each Website's Security

Hackers may steal data when you visit an insecure site. So look for indicators of a secure connection, such as https:// in the address; a lock sign in the browser's address bar; or a green highlight on the merchant's name.



Choose WiFi Networks Carefully

Public WiFi networks usually aren't secured. So only visit trusted websites on public networks. When possible, use your phone's mobile data, which is typically encrypted.