SKIMMER DETECTOR TRAINER

QUICK USER GUIDE

Before You Start - Unpack and completely charge up your Skimmer Detector Trainer unit using the supplied power transformer. Be sure that your Skim Scan™ and BlueSleuth™ units are fully charged and ready to detect skimmers.



Power Requirements - If you are just verifying Skim Scan operation, the Skimmer Detector Trainer will function without any power or charge. If you want to verify BlueSleuth operation and detect bluetooth skimmers, you will need to provide power to your Skimmer Detector Trainer unit or at least make sure its internal battery is charged. The internal battery system powers the unit for up to 24 hours. Push the battery meter button to see how much battery power the unit has stored.



About Skimmers and Skim ScanTM - Push the power button on your Skim Scan unit. The blue LED will light up to verify that the unit has power and is ready to detect skimmers hidden in any DIP (Document Insertion Processor) card readers such as the two readers embedded in the Skimmer Detector Trainer unit. Power to the Skimmer Detector Trainer is not required for this kind of skimmer detection. The same holds true for skimmers hidden inside ATMs or any POS DIP kiosk. Since a hidden skimmer is simply an additional magnetic head, it is always present and always detectable by Skim Scan. The left card reader in the Skimmer Detector Trainer only contains one magnetic reading head and no skimmer. The right card reader contains a skimmer in addition to the normal magentic head.



Skim Scan Skimmer Detection Procedure - Push the power button on your Skim Scan. The LED will turn blue to indicate power. Immediately insert Skim Scan all the way into either card reader as shown - the same way you would normally insert your credit card. As you insert Skim Scan, you will immediately see a green (no skimmer detected) or red (skimmer detected) LED light up and hear an audible beep. Keep Skim Scan fully inserted and wait until all LEDs go dark. With Skim Scan still inserted fully, press its power button (you will see blue LED) and pull Skim Scan back out of the reader to verify the initial detection. Since hidden skimmers are relatively rare in the real world, you should repeat these procedures multiple times when a real hidden skimmer is discovered. This should correct for the small possibility of false skimmer detection due to electrical interference or operator error.



NO SKIMMER DETECTED



SKIMMER DETECTED





Before You Start - Make sure your Skimmer Detection Trainer has power and is turned on. Check the internal battery meter level if you plan to use it in an area that does not have AC power for an extended period of time. Once you are ready to begin detecting bluetooth skimmers, turn on the round, blue backlit bluetooth skimmer power button on the right side of the Skimmer Detection Trainer unit.

About Bluetooth Skimmers and BlueSleuth - Power up your BlueSleuth™ unit and refer to the quick start guide that it shipped with. Once your bluetooth skimmer is tuned on, allow at least 90-120 seconds for the BlueSleuth to detect it. Begin with the unit pointing closely to the Skimmer Detection Trainer card slot on the right side. You may see a list of nearby bluetooth devices (MAC addresses) on the BlueSleuth screen. These will appear in white and are normal, benign bluetooth devices found in most environements. When you see a device listed in red, you have detected the signature of a known bluetooth skimmer (one of many listed in BlueSleuth's skimmer lookup table) found inside the Skimmer Detector Trainer. Note the signal strength of the skimmer (red) in relation to all background bluetooth activity (white). The bluetooth skimmer should always have the strongest signal strength when you are closest to the Skimmer Detection Trainer. Refer to the complete operation of BlueSleuth using its included guick start guide.

Bluetooth Skimmer Detection - Positive identification of a bluetooth skimmer requires more than just the appearance of a device display in red. Law enforcement and/or location managers are tasked with locating and removing every illegal skimmer on every premise they search. This requires physical access to every kiosk and the ability to open each one up in order to physically verify and remove the skimmer(s). Locations such as gas stations and banks typically include multiple adjacent pumps and ATMs. In order to avoid lengthy unlocking and inspection procedures, users must first pinpoint the precise POS kiosk containing a bluetooth skimmer for the entire location by repeating the above steps for each and every kiosk.









