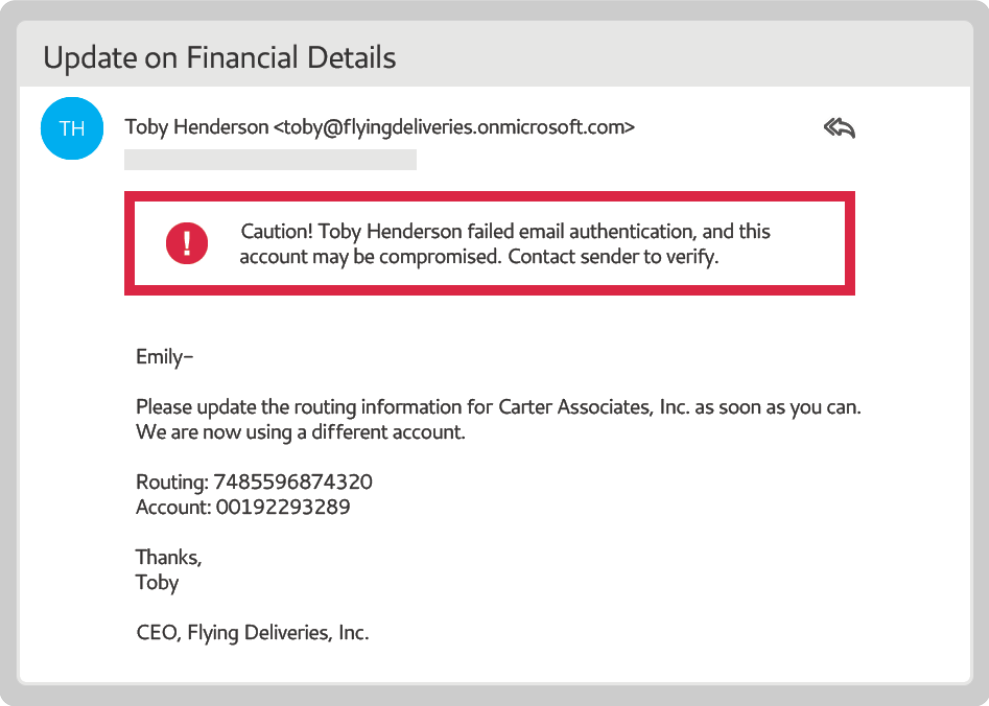
GreatHorn Account Takeover Protection



Identify compromised accounts and block account takeover attempts using biometric authentication

Difficult to Bypass

Authentication is trustworthy and difficult to replicate as it's based on biometric data

Minimally Disruptive

Initial setup and ongoing verification is as simple as typing an email address

Simple Implementation

Administrator roll-out via Outlook plugin – no additional apps or devices

Configurable Actions

Failure actions can be adjusted based on risk tolerance or group – from a simple alert to send prevention

Mobile-Friendly

Supports mobile, desktop, and web interfaces to ensure protection regardless of access method

Compatible with Other Solutions

Use in conjunction with multi-factor authentication or identity access management solutions

GreatHorn Account Takeover Protection provides a low-friction, secondary layer of authentication that's easy to implement, difficult to bypass, and minimally disruptive for employees.

Compromised Accounts: The Enemy Within

The risk of account takeover has increased exponentially – representing up to two-thirds of all phishing attacks today. Yet identifying compromised email accounts can be tricky – often showing up only after there's been financial and reputation damage.

Email accounts increasingly provide greater access to sensitive applications and information. Criminals also use compromised accounts to daisy-chain their way to senior executives with greater access and authority.

A Biometric Solution to Account Takeover

While multi-factor authentication (MFA) can help protect organizations from account takeover attacks, less than 10% have implemented MFA across their enterprise. In addition, MFA isn't effective against cell-jacking, when a device has been left unlocked, or phone-based social engineering.

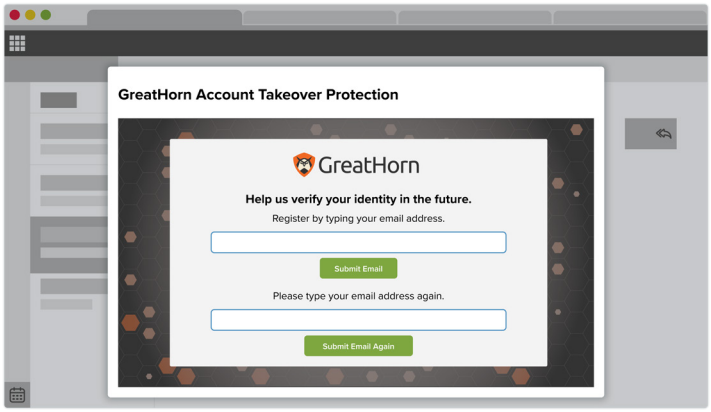
Many solutions that claim to provide account takeover protection attempt to identify account takeover based on behavioral cues. While helpful, such products cannot truly verify the sender's identity.

Simple, Easy Identification

An individual's typing pattern is automatic, always available, and unique. Account Takeover Protection uses machine learning to capture an employee's unique typing pattern on both desktop and mobile devices – analyzing the dynamics of a user's keystrokes, e.g. speed, pressure, and timing between key press and release, but not the keystrokes themselves.

Low-Friction Implementation

Account Takeover Protection is universally deployed across all clients – desktop, mobile, and web – by an administrator without installing additional applications or requiring



complicated user set-up. Employees use their email address for authentication, with separate typing patterns for mobile and computer use. No additional software, hardware, or passwords required.

Visibility, Control, and Early Notification

Administrators can determine how often different groups of employees are challenged – adjusting it based on frequency, time delay, communication pattern anomalies and more.

You can also configure actions based on authorization failures – such as inserting a warning banner to the recipient, removing the message upon send, alerting the security team, or simply logging the event for later analysis. Failed attempts populate into the GreatHorn dashboard providing context for faster incident response.

ABOUT GREATHORN EMAIL SECURITY

Account Takeover Protection is part of GreatHorn Email Security, a comprehensive platform that helps enterprises manage the inherent risk associated with the everyday use of email. GreatHorn's multi-layered approach to email security automatically combines data science, machine learning techniques, and technical analysis with human context to protect organizations before, during, and after a phishing attack.

By treating email security as a risk management function, customers can not only detect and remove more attacks, but also warn users in real-time of potential threats and provide response teams with the tools to limit exposure and minimize risk. As a result, GreatHorn Email Security safeguards cloud email from advanced threats such as business email compromise, impersonations, credential theft, account takeover, and other phishing attacks.