BLOG POST

6 Reasons Social Engineering Is More Successful During Summer Vacation Season

Cybercriminals purposely target users during summer vacations – here's why

AUGUST 18, 2026

Key Points

- While social engineering attacks are a potential hazard for organizations all year, they are especially successful during the summer vacation season.
- Cybercriminals seek to take advantage of key personnel being out on vacation and users being distracted by a number of factors during the summer months.
- Mimecast has compiled six reasons social engineering attacks are more successful during the summer, hoping to arm organizations with the insight needed to help stop these attacks.

Cyberattacks are continually on the rise, becoming more and more sophisticated as time goes on. Organizations attempt to combat these attacks with emerging technology like Mimecast's Human Risk Command Center. And while these solutions can be extremely effective at stopping most attacks, users remain the most vulnerable link in the cybersecurity chain.

Distracted users unknowingly help cybercriminals

Cybercriminals rely on users being distracted, overworked, negligent, and complacent. Each day these threat actors set out to find weaknesses in security at companies of all sizes, all around the world. Sadly, they don't usually have to go far – or wait too long – before human error results in a foothold inside a secure network.

And at few times of the year is this vulnerability greater than during the summer vacation season. Workers are distracted by upcoming time off from work, trip planning, travel, family relationships, financial concerns, and a host of other factors that are especially distracting during the summer months.

In a rush to leave the office to begin a vacation, are emails that should never have been opened being opened? Are links that never should have been clicked being clicked? Are social engineering and other aggressive attack tactics being overlooked?

Six things to look for during summer vacation season

Every year, the summer vacation season proves to be a liability for organizations when it comes to security. Here are six reasons why attacks such social engineering, phishing, and executive impersonations are all more successful during summer vacations:

1. Cybercriminals know people are out of the office and can take advantage of workers being prone to skipping checks and balances when managers and approvers are away.
2. Employees take their work devices with them on vacation, making them more vulnerable to being physically stolen during travel.
3. Cybercriminals take advantage of security lapses in Wi-Fi hot spots when traveling employees connect their devices to unfamiliar and unsecure networks.
4. IT professionals are on vacation, and while cybersecurity is everyone's responsibility, the fact remains that critical system updates and cyber breach remediation can take much longer when IT staff are away.
5. Employees create the biggest summer season threat, human error, in particular errors that can occur when workers are distracted or rushed, making it very easy for cybercriminals to quickly build the trust they need to then ask for sensitive information, or even worse, a fraudulent transaction.
6. Employees share information about their vacations online, arming cybercriminals who might be tracking them with exactly what they need to know to exploit security weaknesses through pretexting and other social engineering attacks.

The bottom line

Social engineering is a growing issue in cybersecurity, but the tools to counteract this practice are on hand. Holistic email security policies, when paired with strong employee awareness training and security behavior management through Mimecast Engage and a human risk command center, can also help security teams stay on point and evolve their defenses to block the attackers' latest tactics.