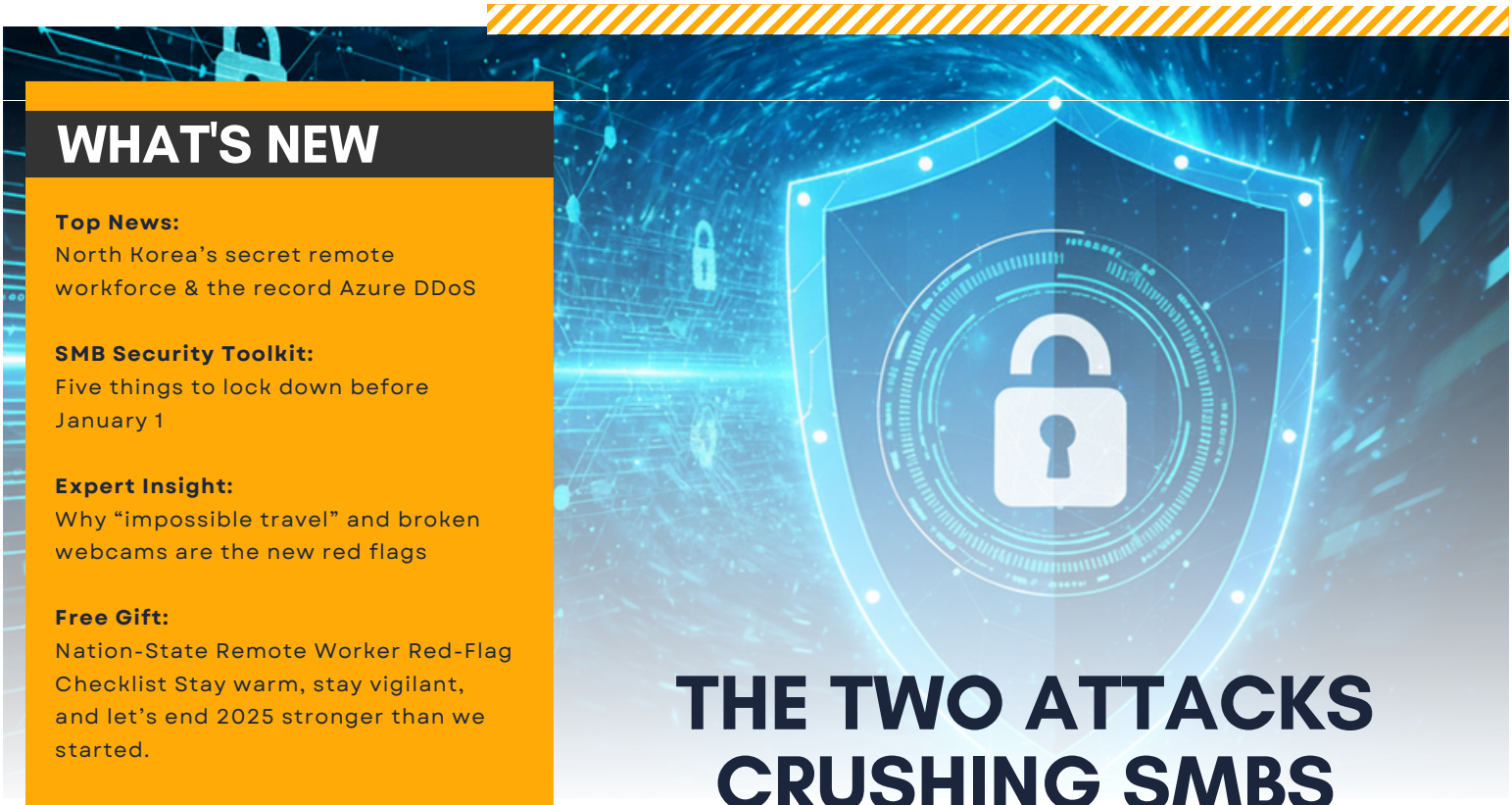
# DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



## WHAT'S NEW

**Top News:**
North Korea's secret remote workforce & the record Azure DDoS

**SMB Security Toolkit:**
Five things to lock down before January 1

**Expert Insight:**
Why "impossible travel" and broken webcams are the new red flags

**Free Gift:**
Nation-State Remote Worker Red-Flag Checklist Stay warm, stay vigilant, and let's end 2025 stronger than we started.

**Black Belt Secure** offers comprehensive cybersecurity solutions to protect your personal and business data from online threats.

*This monthly publication is provided by Peter & The Black Belt Secure Team*

## OUR MISSION:

**To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients**

# THE TWO ATTACKS CRUSHING SMBS

## LOCK DOWN BEFORE 2026

Greetings, Defenders!
December is here, and while most teams are winding down for the holidays, nation-state hackers and botnet operators are ramping up.

This month delivered two wake-up calls that hit SMBs harder than any enterprise:

- North Korean IT workers have been living inside hundreds of U.S. companies (some for years)
- The largest DDoS attack ever recorded just slammed Microsoft Azure at 15.7 Tbps.

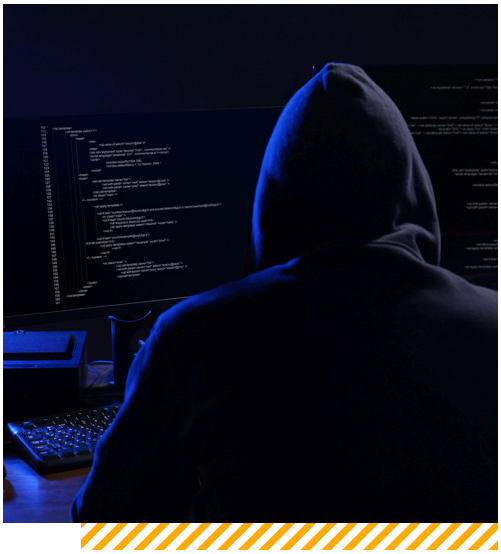
The lesson? Remote work and the cloud are now the two biggest doors attackers walk through—and for most small and mid-size businesses, those doors are standing wide open.

Attackers aren't smashing windows anymore. They're logging in with stolen credentials, hopping from home laptops to your SaaS admin consoles, and quietly exfiltrating data while everyone's on Zoom. Every major breach this year—MGM, Snowflake, Okta, Microsoft 365—started the exact same way: valid credentials, no malware required.
In this edition, we break down exactly what happened, why it's a direct threat to you right now, and give you five dead-simple actions you can finish before New Year's Eve that will slam those doors shut faster and harder than most companies manage with a six-figure budget.

*continued on page 2...*

*...continued from cover*

# NOVEMBER'S CYBER HEADLINES WHAT SMBS NEED TO KNOW



Here are the two stories that dominated threat intel channels last month—and the direct impact on your business:

### North Korea's Secret Army Inside 600+ U.S. Companies

On November 13, 2025, five American facilitators pleaded guilty in federal court to orchestrating the largest remote-worker identity fraud scheme in U.S. history. Over 6,000 North Korean IT operatives used stolen Social Security numbers, deepfaked video interviews, and paid U.S.-based "laptop farm" operators to appear as legitimate remote employees. They infiltrated more than 600 companies—including Fortune 500 retailers, defense contractors, and critical infrastructure providers—earning $100,000–$200,000 salaries with full administrator privileges and unrestricted source-code access. Every dollar was wired back to Pyongyang, directly funding ballistic missiles and nuclear development while insiders quietly mapped corporate networks for future sabotage.

**SMB Lesson:** If your "new senior DevOps hire" never enables their camera, works only midnight-to-8 a.m. U.S. time, and demands the $6,000 MacBook be shipped to a random residential address in Ohio or New Jersey, you may already have a DPRK state employee on payroll.

### Record 15.7 Tbps DDoS Slams Microsoft Azure

The newly discovered Aisuru botnet, an aggressive evolution of the Turbo Mirai family, launched the largest DDoS attack ever documented: 15.72 terabits per second and 3.64 billion packets per second sustained for over 20 minutes against Microsoft Azure regions in November 2025. Powered by more than 500,000 compromised IoT devices, DVRs, smart fridges, and poorly secured home and business routers across 180 countries, the assault dwarfed previous records. Microsoft's global scrubbing centers absorbed the flood, but Aisuru remains active and is still infecting thousands of new devices daily.

**SMB Lesson:** You don't need to be Microsoft to get hit—these bots spray everything. If your website or VPN is exposed to the internet without always-on DDoS protection, you're on the menu.

### Quick Stat

According to a Verizon DBIR 2025 preview, 68% of organizations hit by ransomware this year had zero multi-factor authentication on remote access points such as VPNs and RDP. Of the remaining 32% that did have MFA enabled, the vast majority of breaches still began with employees clicking phishing links or approving fraudulent MFA prompts.

**Moral:** MFA helps, but it's not a silver bullet if your people remain the weakest link.

# SMB SECURITY TOOLKIT

## *FIVE THINGS TO DO BEFORE JANUARY 1*

Knock these out in the next two weeks and you'll sleep better over the holidays:

### Tip 1: Force MFA on every remote worker – no exceptions, no "grandfathered" accounts

As of today, enforce hardware keys or push-based MFA with number matching on every single account that can touch email, VPN, RDP, GitHub, AWS, or HR systems. Free options include Microsoft Authenticator (built-in), Duo Free (up to 10 users), or Google Authenticator with TOTP seeds.

**Quick win:** enable "number matching" and "location + device context" in Microsoft/Entra push notifications so sleepy employees can't blindly approve logins at 3 a.m. Without this, you're literally begging to be the next Verizon DBIR statistic.

### Tip 2: Stop shipping company laptops to home addresses for new remote hires

New rule: all new laptops ship only to a company office or verified co-working space, or the employee must pick up the device in person, present government-issued photo ID that exactly matches the HR record, provide a live selfie on the spot, and physically sign the asset receipt in front of a company representative or notary. The FBI publicly stated this one rule would have prevented 90% of the North Korean IT-worker fraud cases. No exceptions for "trusted" recruiters or "senior" titles. If the candidate ghosts after hearing this requirement, you just dodged a state-sponsored operative.

### Tip 3: Run an "impossible travel" report this week

Open Microsoft 365 Defender → Entra ID → Sign-in logs (or Okta System Log, Duo Admin Panel, Cloudflare Zero Trust, or your VPN concentrator, or SIEM). Filter for successful interactive logins where the same user appears 3,000+ miles / 4,800+ km apart in under 60 minutes (classic example: Dallas at 8:02 p.m. CST, then Seoul at 8:47 p.m. KST). North Korean workers using U.S. laptop farms trigger this flag literally every single shift. Quick win: deploy a real-time Conditional Access Policy, Okta Sign-On Policy, or SIEM rule that instantly blocks and forces step-up authentication (FIDO2/phish-resistant MFA) the moment any user hops continents in under two hours. Run the historical report today—you will be shocked, possibly horrified, at what's already hiding in your logs.

### Tip 4: Confirm your backups are immutable & air-gapped

Ransomware crews deleted 43% more backup repositories in Q4 2025 than Q4 2024 because most "immutable" features are easily bypassed with stolen admin tokens. Stop trusting vendor checkboxes. Personally verify you have real write-once storage: AWS S3 Object Lock with default retention + governance mode bypass disabled, Azure Blob immutable policies with secured legal hold, Veeam 3-2-1-1-0 on a hardened Linux repo with immutable flag, or old-school weekly LTO-9 tapes/encrypted USB drives rotated to an offsite safe. Test full bare-metal restores every month with a different admin account. If the same compromised credentials that own your production environment can also reach and delete your backups, you are 100% guaranteed to pay the ransom.

### Tip 5: Book your 2026 penetration test now

We still have three December slots open. Reply "TEST" to audit@blackbeltsecure.com and we'll lock one in for you.

BLACK BELT SECURE
*Defend Today, Thrive Tomorrow.*

# EXPERT CORNER:

## THE NEW RED FLAGS HR AND IT MUST SHARE

- Webcam never works (ever)
- Refuses in-person meetups or notary verification
- Lives in a high-cost city but wants payroll sent to a different state
- Logs in at perfect 9-5 U.S. hours… from a time zone 13–14 hours ahead

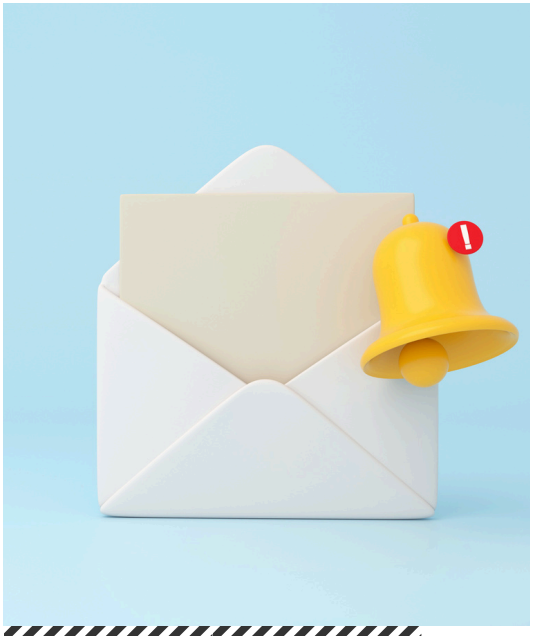
**If two or more of these match someone on your team, escalate immediately.**

### Your Free End-of-Year Gift

Download our brand-new one-page PDF:
"Nation-State Remote Worker Red-Flag Checklist"
The exact 17 signals the FBI used to catch these guys.
→ blackbeltsecure.com/nk-checklist

## ASK THE EXPERT

**Got a question? Email us at info@blackbeltsecure.com!**



# DECEMBER ACTION ITEMS

- Set a Google Alert for your company name + "breach"
- Run that impossible-travel report before the office Christmas party
- Forward this newsletter to one colleague and we'll send both of you the checklist + a $500 credit toward any 2026 assessment

Want a free dark-web scan + 15-minute 2026 planning call?
Reply "2026" or book here: audit@blackbeltsecure.com.

*The Black Belt Secure Crew*

P.S. 2025's biggest lessons (and the three threats coming in 2026) drop in the January issue. Make sure you're still on the list!