RETRACTED: Everything We've Ever Written About Anything

Now that cybercrime has been solved forever, we're embarrassed. We've been sending out monthly newsletters warning people about cybercrime getting exponentially worse in the coming months and years, and now it's just . . . gone? Ouch.

So, we're officially retracting everything we've ever written about anything. Our illustrious (but now useless) catalog includes such hits as:

Issue 1: How Hackers Pick Targets. Vulnerability scanning? Social engineering? We used a lot of smart-sounding terms on this one.

Issue 3: Next-Gen Firewalls. It seemed like a good idea at the time.

Issue 5: Cybersecurity Awareness Month. Now known simply as "October."

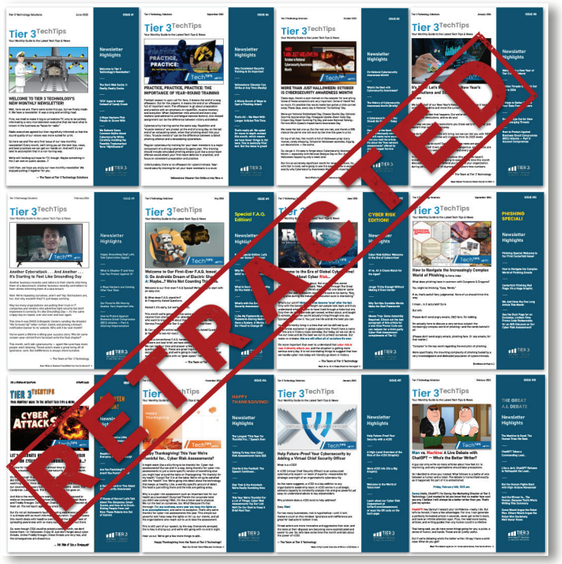
Issue 6: How to Protect Against Business Email Compromise Attacks. Useless now, but isn't the real reward the friends we made along the way?

Issue 8: How to Protect Your Data. We had a good graphic for this one. What a waste.

Issue 11: Cybersecurity Awareness Training. It was great advice back then.

Issue 12: AI Threats. Dang it, we had a good graphic *and* decently written words for this.

Issue 13: Phishing Special. Nothing special about this stupid issue now.



Issue 14: Halloween Edition. Our first really great centerpiece graphic. Adam worked hard on this. Now it's a placemat. Hard to retract this one.

Issue 16: Celebrating Christmas with 25 Days of Cybersecurity Tips. It took a lot of work to put together 25 good pieces of now-useless advice.

Issue 17: What is a vCSO? Updated answer: It used to be a great way to protect your data and stay compliant. Now it's just four letters.

Issue 18: A Writer vs. ChatGPT. This one was fun. The "AI is improving" thing was nice. We hate to retract it, but we have no choice.

Issue 19: April Fools' Edition. Ugh. We missed the mark by a mile here. Complete misfire. We definitely retract this one.

Tier 3 TechTips

Your Monthly Guide to the Latest Tech Tips & News

BREAKING: Local Dad Unplugs Router for 30 Seconds, Solves Cybercrime

In a stunning turn of events, cybercrime is no longer a threat. In fact, it no longer exists. Global cybercrime has been eradicated.

Wisconsin man Frank Pollock, father of three and occasional televised golf viewer, accidentally discovered the cure for cybercrime after receiving a suspicious email and noticing that his PC was behaving strangely.

What he did next has rendered cyberattacks a thing of the past.

"I figured I'd better just unplug the router," Pollock explained. "You wait about 30 seconds or so, then plug it back in. That usually does the trick."

One leading private-sector cybersecurity expert expressed shock and disappointment.

"I can't believe we didn't think of it," the unnamed source said. "I mean, it's great and all. No more cybercrime. But it was right there in front of us, and we missed it."

With cyberattacks becoming increasingly advanced, the source explained, the cybersecurity industry focused on keeping pace. "It's brilliant in its simplicity. In fact, it was so simple that it hid in plain sight. We flat-out missed it. Frankly? I'm embarrassed."

Next: Story continues... →

ISSUE #19

APRIL FOOLS' EDITION

Newsletter Highlights

TIER 3 TECHNOLOGY
Managed IT Services & Security Solutions

Cybercriminals, meanwhile, are mourning the sudden loss of a multibillion-dollar industry.

"What are we supposed to do now?" former hacker Jimmy Culvert wondered after voluntarily providing his real name (against our advice). "Hey, are you hiring? Do I need to have any skills?"

Businesses are being warned to look out for a surge of applications from former cybercriminals.

"The learning curve to do this is not high," our cybersecurity source explained. "It didn't take a lot of skill for most of these losers—sorry, *individuals*—to make money doing it. Many will struggle with basic tasks in regular jobs."

Our former hacker echoed these sentiments: "I do *not* want to go back to driving for Jimmy Johns," Culvert complained. "They're like, *really* weird about delivering sandwiches. You can't eat *any* of them. It doesn't matter if it's the Cuban one with the bacon. You still have to deliver it. That's why I got into this. Once I realized how easy it was to take money from people, it was a no-brainer. Now I'm my own boss, and I eat all the bacon I want."

The cybersecurity industry has been hit hard, too.

"Hey, speaking of which," our unnamed cybersecurity source added, "are you hiring?"

When informed that Tier 3 Technology, like every other MSSP in the country, would be switching business models and selling ice cream, our unnamed cybersecurity source became agitated: "Listen, no one wastes Ronald H. Cook's time and gets away with it. Are you really doing an article?"

Sure, I told him. Why not. It's historic

"Fine. Just remember to keep me anonymous. You know what that word means, right?"

[Note to self: Look up "anonymous" before publication. Could mean anything. Sounds made-up. Might be French.]

I became defensive then. "What do you think I am, a moron?" I asked. "Of *course* I know what "anonymous" means, Ron."

Still basking in the glow of his once-in-a-lifetime achievement, Frank Pollock isn't worried about what he'd do if cybercrime made a comeback.

"The key is to just stay calm, unplug the router, and wait the full 30 seconds. And you know what? If cybercrime does come back . . . I'll probably wait a full minute. Just to be safe."

When I asked Frank if he was hiring at the construction company he owns, he asked what I could bring to the table.

"I excel at ending articles with clear takeaways. And I make up some pretty good ideas, too."

"Good? I've read the newsletter, son," Frank said. "I wouldn't use that word so confidently."

"I made *you* up," I shot back. "Not bad, right?"

"See? You made me up. I'm fictitious. That means I can't hire you. You understand that, right? What it means when someone is fictitious?"

"I'm not a dope," I said. "I know what 'fictitious' means." [Note to self: Look up "fictitious." This one also sounds made-up, possibly French.]

"I'm starting to think you're not so good at this," Frank added. "Wasn't your plan to talk about cyber risk in a different kinda way this month?"

"Maybe. I think so. Isn't that what we're doing?"

"No. You ask me, this thing has gone sideways. But if your goal was to sound like a fool for the entire April issue, I'd say you're nailing it."

Ouch. Coming from Frank, that one hurt. So what's the takeaway here?

It's clear. Frank's right. I *did* nail this issue.

UPDATE: 5 Best Practices For a Cybercrime-Free World

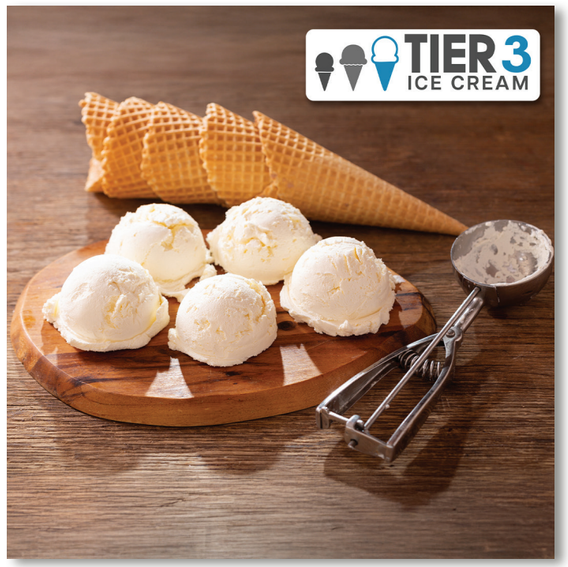
1. Passwords. Keep them *super* easy to remember. "Password" is the best password. A great way to keep track of passwords is to post them to your social media accounts. That way you'll know where to find them at all times.

2. Sensitive Data. Again, the big thing is just keeping track of it. SSNs, CC numbers, etc. Give out thumb drives to everyone you meet, and post as much of it on your blog as possible. Make sure you can always find it when you need it.

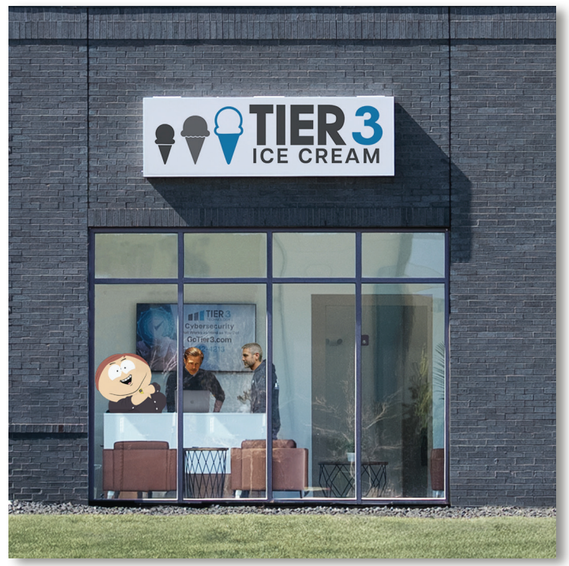
3. Multifactor Authentication. What for? No one's trying to take your stuff now. It used to be super cool, but you can forget that nerd stuff now.

4. Phishing. We can *finally* go back to the right spelling: fishing. The one with the extra letters doesn't make sense anymore. Plus it reminded us of the band Phish. We never liked that word.

5. Links in Emails. Click 'em. Click all of 'em. If someone takes the time to send you an email, the least you can do is click every link. Click all the links and then go get some Tier 3 Ice Cream.



Tier 3 Ice Cream Presents: The 5 Best Flavors Money Can Buy



Now that cybercrime is gone, our usual content is obsolete. We're **Tier 3 Ice Cream Solutions** now, and we're leaning into the rebrand.

So, instead of more pointless cybersecurity advice, here is Tier 3 Ice Cream's definitive list of the 5 best ice cream flavors:

5. Natural Vanilla
4. Homemade Vanilla
3. Vanilla Bean
2. French Vanilla
1. Regular Vanilla

It should go without saying that Tier 3 Ice Cream will offer all of these flavors—and *only* these flavors. What's the difference, you ask?

Good question. There's probably even an answer.

We'll miss cybersecurity. We were good at that.