(October 24th, 2024)

If you know someone who would benefit from being an Insider, feel free to forward this PDF to them so they can sign up here.

Note: As an Insider, you can read all prior Insider newsletters here.

Quick Tips for our Insider friends!

This mini-newsletter comes to you from Camp Savage where we're still hard at work putting in infrastructure in preparation for building some living structures in November which will let us be up here more easily over winter. With a predicted La Niña winter, it's going to be cold and wet (well, colder and wetter)!

Black Friday Super-Sale!

It's the time of year again where companies do crazy sales on the day after Thanksgiving in the US, and we're doing the same!

Starting at 4pm PST on Thursday, November 28th, we'll be offering our **lowest prices ever** for our signature Blackbelt bundle with more than 158 hours of top-quality training (plus all our SQL Server 2022 update/Q&A recordings):

- **One-year access to the Blackbelt bundle: US$990**
- ***Lifetime* access to the Blackbelt bundle: US$1,895**

From Monday, December 2 12:00am GMT (starting at 4pm PST on Sunday, December 1) and until 12:00am GMT December 17 (ending at 4pm PST on Monday, December 16), we will offer lower than our regular prices but not as deep of discounts as Black Friday. If you've already purchased a bundle or class once, you can purchase the one-year access for a second time and we'll convert your existing access into lifetime access, by removing all the expiration dates.

**** New in this newsletter:** We'll also have the IE0 training class for Accidental and Junior DBAs (over 32hrs; not included in the Blackbelt bundle) on sale!

- **One-year access to IE0: US$795 (usually US$1,695)**
- ***Lifetime* access to IE0: US$1,495 (usually US$3,495)**

We're going to do mini-newsletters each week through October and November so stay tuned as I'll be adding some more sale prices on courses and bundles!

Any questions, please let me know.

Book Review

One of the books I read earlier this year was *Moll Flanders* by Daniel Defoe – a classic I've wanted to read for a long time. From Amazon: "Written in a time when criminal biographies enjoyed great success, Daniel Defoe's Moll Flanders details the life of the irresistible Moll and her struggles through poverty and sin in search of property and power. Born in Newgate Prison to a picaresque mother, Moll propels herself through marriages, periods of success and destitution, and a trip to the New World and back, only to return to the place of her birth as a popular prostitute and brilliant thief. The story of Moll Flanders vividly illustrates Defoe's themes of social mobility and predestination, sin, redemption and reward." Highly recommended!

Ponderings…

(Following on from the ransomware attacks editorial last week, I'm re-running an editorial I last ran five years ago about considering ways a hacker might use phishing or social engineering to gain access to your environment – enjoy!)

Back in April 2014 I wrote an editorial in the newsletter focused on security, with my older TechNet Magazine article as a base. As I was reading the book *@War: The Rise of the Military-Internet Complex*, it struck me that security checklists and security reviews of SQL Server environments are all well and good, but there are a few missing things that I think are worth considering.

For instance, does your company provide training or guidance on recognizing and avoiding phishing emails? Phishing is the word describing an email that entices the recipient to open it and maybe click a link, which then installs some malware on the computer. This could be something that logs keystrokes and sends them to another system on the Internet. If a DBA unknowingly installed such malware on a personal laptop, say, and then connected to a work system, the hackers could capture the DBA's login credentials.

Such phishing emails could be cleverly targeted, especially if hackers are going after a specific company and make an email look like it's coming from a source the DBA trusts. The @War book has several descriptions of this being done to companies like banks and defense contractors. You'll likely have received emails like that, purporting to come from Microsoft or PayPal or some other company you recognize, and urging you to click a link to fix something to do with your account.

A way to test people in your company would be to create a fake email with a link that takes them to a web page showing that they've clicked something they shouldn't have and to be wary in

future – or just to keep track of what proportion of recipients in the company were fooled into clicking the link.

Another thing to be wary of is social engineering. This is where a hacker calls someone on the phone, pretending to be someone who needs some information that can help them break into a computer system, and fools the person into giving that information out. This wasn't in the @War book, but is something I've read about being used many times in the past, and is a relatively common technique used by phone scammers.

Finally, one of the things you might consider for your company is engaging the services of a third-party company that does penetration testing. These people will deliberately try to hack into your environment, with your permission, to discover security weaknesses that you can then patch before a malicious hacker tries to break in.

Sometimes this is known as *ethical hacking*, and you can actually learn how to do it yourself. For instance, on Pluralsight there is a set of courses that will help you learn how to think about security from the attacker's perspective and assess your own environment for security flaws. Check them out here.

Call to Action

If you're responsible for databases that contain any information that you don't want someone to have unauthorized access to, you need to make sure that your security doesn't have any problems. That includes making sure that the users are educated about ways that they can be duped into giving out info or installing malware, and testing your system's defenses to see if they can be broken. You can be sure that someone out there will try to get in sooner or later.

#TBT

(Turn Back Time…) Blog posts we've published since the previous newsletter plus some older resources we've referred to recently that you may find useful.

The TBT this time is about identifying and fixing esoteric query plan performance issues, and Joe recorded four excellent courses on this that are entirely relevant to all versions of SQL Server:

- *SQL Server: Common Performance Issue Patterns*
- *SQL Server: Common Query Tuning Problems and Solutions – Part 1*
- *SQL Server: Common Query Tuning Problems and Solutions – Part 2*
- *SQL Server: Troubleshooting Query Plan Quality Issues*

I hope you find these useful and interesting!

Upcoming SQLskills Events

Given how little changed with SQL Server 2022, we decided to record a series of updates relevant to our class material rather than running full classes. These are done as part of our Blackbelt Base Camp series and are available in our shop, our free with a Blackbelt bundle.

With our streaming system, you can now choose to attend a live, online event or purchase a recording to watch at your leisure, either individually or as part of a bundle. And all attendees of live events get lifetime access to the class recordings too!

To help your boss understand the importance of focused, technical training, we've also added a few items to help you justify spending your training dollars with us:

- Letter to your boss explaining why SQLskills training is worthwhile
- Community blog posts about our classes
- Immersion Event FAQ

You can get all the details on our training options page or just go directly to our shop.

Summary

I hope you've enjoyed this issue – I really enjoy putting these together. If there's anything else you're interested in, I'd love to hear from you - drop me a line.

Thanks,
Paul

Paul@SQLskills.com