

DECEMBER 2023

TECHNOLOGY INSIDER



Should your
business
follow
Google's
security lead?



Your monthly
newsletter, written
for humans!

DID YOU KNOW...

not to download
third party
apps?

New research has found that an Android app is actually a trojan (a type of malware) that can record your video and audio calls. The SpyNote banking trojan is typically delivered by a phishing SMS, and once installed, it's very hard to get rid of.

How do you avoid it?
Simple. Only download
apps from official app
stores - never via third
parties.



Google has introduced a new security strategy - but is it right for your business?

It has put some employees on a cyber diet, restricting their internet access to limit potential threats.

On the surface, it sounds like a smart move. Google's approach is like building a taller fence around your house to keep out burglars.

By reducing internet connectivity, they're effectively shrinking their digital footprint and making it harder for cyber criminals to find a way in.

But is it foolproof?

Well, not exactly.

While this strategy does limit external threats, it doesn't entirely eliminate the risk.

Think of it this way: you've built a towering wall around your house, but your teenager leaves the back gate open. Similarly, internal systems might remain connected to other devices that can access the internet, providing a potential entry point for cyber threats.

In other words, you can't just focus on keeping things out.

Yes, there are very real threats from external hackers using all sorts of techniques like phishing, zero-day attacks, and malware. But the security industry often overlooks significant threats from within the organization's network.

Research shows that insider threats account for 62% of all security breaches. These insiders - disgruntled employees, careless staff, or malicious actors - often have legitimate access rights, intimate knowledge of the system, and can bypass traditional security checks. It's like having a burglar who knows where you hide your spare key.

So, what's the takeaway?

While Google's strategy has its merits, it's not a one-size-fits-all solution. Just as you wouldn't wear shoes that are too big, your business needs a cyber security strategy tailored to fit its unique requirements. A robust cyber security strategy should focus on both external and internal threats and have measures in place to mitigate risks from all angles, including users.

Our advice? Instead of simply following in Google's footsteps, consider your own business's needs and vulnerabilities. And of course, if you need help with that, get in touch..

It's time to turn the tide on phishing attacks

Phishing attacks have reached record highs this year. In the third quarter of 2023, **phishing attacks skyrocketed by a staggering 173%, compared to the previous three months.**

And malware? It's not far behind, with a 110% increase over the same period.

Let's put this into perspective. Imagine you're on a quiet beach, enjoying the sun and the surf. Suddenly, the tide starts to rise rapidly. Before you know it, your picnic basket is floating away, and you're knee-deep in water. That's what's happening in the cyber world right now.

According to a report, the 'phisherfolk' group were most active in August, casting out more than 207.3 million phishing emails. That's nearly double the amount in July. September wasn't much better, with 172.6 million phishing emails.

But who are these cyber criminals targeting? Old favorites Facebook and Microsoft continue to top the charts, with Facebook accounting for more phishing URLs than the next seven most spoofed brands combined.

So, what's the bottom line here?

Your business could be next.

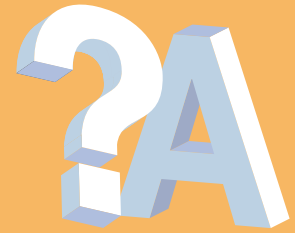
Phishing attacks are like a rising tide, and if you're not careful, they can quickly sink your business. They target everyone - from tech giants to financial institutions, and even government agencies. The question is - are you prepared?

Take a moment to consider the authenticity of emails. Are they from a trusted source? Do they contain suspicious links? Are they asking for sensitive information?

Make sure your employees are aware of the risks. Encourage them to think twice before clicking on a link or downloading an attachment. After all, a moment's hesitation could save your business from a devastating cyber attack.

And don't forget about integrated email security solutions and phishing awareness training. They could be the thing that best help you prevent an attack.

So, as the tide of phishing attacks continues to rise, remember - it's better to be safe than sorry. If you need any further help or advice, get in touch.



Q: If I accidentally close a tab in Chrome, is there an easier way to get it back than searching it up again?

A: Yes, you can bring back the closed tab with a simple keyboard shortcut. If you're using Windows, ChromeOS or Linux it's CTRL+Shift+T; for Mac it's CMD+Shift+T.

Q: I'm finding ChatGPT is not giving me great answers and is inaccurate - what am I doing wrong?

A: You're probably not being specific enough with your question. Also check your question for typos and slang... too many and you won't get great responses.

Q: I'm fed up having to minimize my windows when I want to look at my desktop - surely there's an easier way?

A: If you're using Windows, there is! Look all the way to the bottom and right, beyond the date and time and you'll find a little sliver of a secret button. Click it to minimize all your open windows at once, then click it again to bring everything back.

Business gadget of the month

Logitech Wireless Ergonomic keyboard

When you spend hours at your computer, it's not just your eyes that get tired. Your hands, wrists and shoulders can begin to ache, and you may even develop issues like repetitive strain injury.

This Logitech Wireless Ergonomic keyboard is the answer you've been looking for. It lets your hands move in a more natural way, reducing stress and increasing comfort.

\$213.98 from Amazon.



This is how you can get in touch with us:

CALL: 888.363.3366 | EMAIL: Ask@BeckITSystems.com

WEBSITE: <https://www.BeckITSystems.com>



BeckITSystems[®]
Inc.