NOVEMBER 2023

# TECHNOLOGY INSIDER


*Your monthly newsletter, written for humans*

## Three cyber security threats your team MUST know about

**Your employees are your main line of defense in cyber security, and their training is as crucial as the cutting-edge tools in which you have invested. Are you overlooking this vital element?**

We strongly advise you make an ongoing commitment to regular cyber security training for every single one of your team. That means keeping them up to date on the latest cyber threats, the warning signs to look out for, and of course, what to do should a situation arise.

If you are not already doing that, arrange something now.

While you wait, here are three urgent cyber threats to address right away:

**Admin attack:** Email addresses like "info@" or "admin@" are often less protected due to perceived low risk. But several teams may require access to these accounts, making them an easy target. Multi-factor Authentication (MFA), as simple as using a smartphone, can double your security. Use it wherever possible.

**MFA fatigue attacks:** MFA can feel intrusive, leading employees to approve requests without scrutiny. Cyber criminals exploit this complacency with a flood of fake notifications. Encourage your team to meticulously verify all MFA requests.

**Phishing:** Phishing remains a top threat. Cyber criminals mimic trusted sources with deceptive emails. Teach your team to inspect email addresses closely. Implementing a sender policy framework (SPF) can also improve your protection.

Cyber security training doesn't need to be tedious. Try simulated attacks and think of them like an escape room challenge—fun yet enlightening. It's about identifying vulnerabilities, not fault-finding.

Don't exclude your leadership team. They need to understand the response plan in case of a breach, much like a fire drill.

**Training your staff is not just smart — it's crucial. If you need help getting started, get in touch.**

## DID YOU KNOW...

### Edge is stripping features to keep up with Chrome?

In another bid to tempt Google Chrome fans over to Edge, Microsoft is removing features.

Sounds counterproductive, right? But some of its less popular (read 'failed') features have left the browser a little bloated and overcrowded. These are the features that are being deprecated: Math Solver, Picture Dictionary, Citations, Grammar Tools, and Kids Mode.

**Bet you haven't heard of them, let alone used them?**

# 5 habits your smart remote workers should have

Remote work has become a way of life very quickly, hasn't it? Loads of businesses and their people are reaping the rewards of flexibility and convenience.

But it also brings cyber security challenges that demand your attention. Of course, this should always be a concern, but when you have employees working from home, a coffee shop, or anywhere else for that matter, you need to make sure they are making wise decisions that put the security of your data at the forefront.

**These are 5 habits your remote workers should adopt straight away.**

1. **Choose your work location wisely**
   Working from a favorite coffee shop or a picturesque park may seem like a dream come true, but it can expose you to more cybersecurity risks. Over-the-shoulder attacks, where cyber criminals discreetly snoop on your screen in public spaces, might seem unlikely, but they have real potential to lead to data breaches. Employees should choose to work in quieter, private settings to minimize this risk.
2. **Beware of public Wi-Fi**
   Public Wi-Fi networks are a common breeding ground for cyber threats. If someone must work from a public place, they should always avoid connecting to public Wi-Fi. These networks can be less secure and make you vulnerable to hacking. Instead, use your cell phone's hotspot for a safer internet connection.
3. **Invest in security software**
   Be sure to include anti-malware and password management software. This serves as a protective shield against malware and cyber attacks. It is a valuable addition to both company-provided and personal devices. Not only does it safeguard business data, it can also shield your personal information, such as credit card details and sensitive documents.
4. **Keep everything updated**
   Regularly updating all your devices is not just about gaining access to new features; it also helps your devices and data stay secure from common threats. Software updates contain crucial security fixes that patch vulnerabilities. Remember, it's not just laptops and phones that need updating, but also routers and any IoT (Internet of Things) devices connected to your network.
5. **Manage household risks**
   Even within the confines of their homes, computers hold sensitive business information. If your employees have housemates, children, or other family members sharing their space, ask them to consider implementing parental controls to prevent accidental data breaches. Ideally a business computer should be used for business activity only.

**By adopting these smart habits, as well as taking the right security measures, you can let your people enjoy the benefits of remote work – while everything stays secure and safe.**

**If we can help keep your remote set-ups secure, get in touch.**




**Q: I'm still using the original version of Windows 11 (21H2), should I upgrade?**

A: Yes! Upgrade to 22H2 as soon as possible. Support for 21H2 ended last month (October 2023). That means there will be no further security updates and you may be at increased security risk.

**Q: I've had an email to say a recording of a Video meeting has expired and been deleted. Is there any way I can recover it?**

A: Don't panic. Go to your Recycle Bin, find the recording, and hit "restore". Remember though, you only have a 90 day window to do this. Once the recording is recovered, it is no longer subject to automatic expiration dates.

**Q: Will Google penalize my website if I use ChatGPT?**

A: No. There's no reason to worry about Google penalties when using ChatGPT for your website content. Chatbots don't negatively affect the SEO of your website. But do get a human to review everything written by an AI, to ensure it reads well, is factually correct and makes sense.

**Business gadget of the month**

## Full HD laptop screen extender

Work on a laptop, but love the functionality of multiple monitors? Here's a handy portable solution that will keep you productive wherever you choose to work.

This KEFEYA laptop screen extender just plugs and plays, leaving you free from fiddling with cables or stressing over setting up complicated software. It means you can work across a range of apps at the same time, or even share your screen with customers more easily.

**$287 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.