

CYBERSECURITY WELLNESS

How to build healthy digital habits



THIS MONTH'S TOPICS:

Healthy Cybersecurity Habits

Habits to stay secure online

Digital Detox

Cleaning up your digital spaces

Scam of the Month:

Image-based Scams...

Monthly Game Time:

Spot the Scam

When we think about healthy habits, we often focus on fitness, nutrition, and mindfulness. But what about your digital life? Just like your physical and mental well-being, your online presence needs care and attention. It's time to detox, strengthen, and sustain your digital wellness!

In this month's newsletter we'll explore practical ways to adopt healthy cybersecurity habits that will keep your data secure, devices optimized, and stress levels low. We will also discuss healthy password practices and ways to detox your digital spaces.

Healthy Cybersecurity

Tips

Refresh Passwords

If a breach or potential exposure has occurred, refresh the password to avoid further exposures.

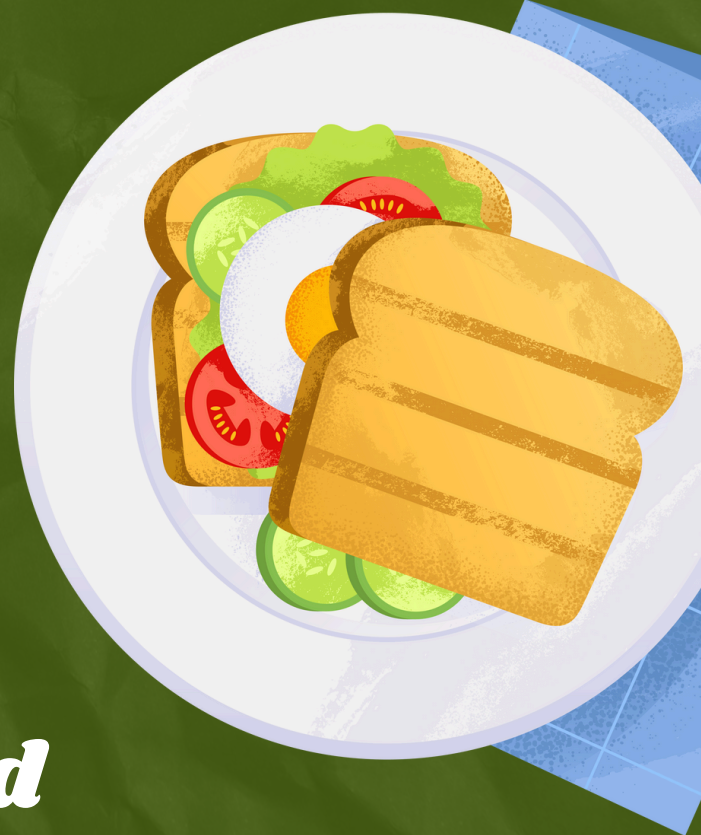
Health 
is wealth

Add Some Variety

Using the same password is like eating only one food. Your digital life needs a variety of passwords to thrive.

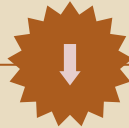
Plan Ahead

Plan ahead when it comes to cybersecurity. Make sure your prevention measures, like backups and remote wiping, are set up.



DIGITAL DETOX

A MESSY DIGITAL LIFE CAN BE JUST AS OVERWHELMING AS A CLUTTERED HOME. IT'S TIME FOR A CYBERSECURITY CLEANSE!



Declutter your digital life by deleting any files you no longer need and getting rid of unused apps. This can reduce the risk of sensitive data being exposed.

KEEPING FILES AND DEVICES ORGANIZED CAN INCREASE PRODUCTIVITY AND IN TURN, HELP YOU AVOID SECURITY FATIGUE AND STAY SAFER ONLINE.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Sam, a warehouse manager, is always checking emails to stay on top of shipments. One afternoon, he receives an email titled "Delivery Attempt Failed - Action Required" from what appears to be a trusted courier service. The email contains no text or even links, just an image mimicking the courier's branding with a QR code to "resolve the issue."

Without hesitation, Sam scans the code. It directs him to a professional-looking webpage asking him to confirm his warehouse's address and log in to his company's account with the courier service. Sam enters his credentials. Within minutes, the scammers use those credentials to access the company's account, rerouting several high-value shipments to their own drop-off locations. It wasn't until a supplier called to ask why their packages had been redirected that Sam realized he had been scammed.



Did you spot the red flags?

- ▶ Sam should not have scanned a QR code from an unsolicited message, as they can be used to disguise malicious links.
- ▶ Sam should have validated the request with the company through another communication method.



In image-based scams, the email might look slightly stretched or blurry and might use colors that seem slightly off from the brand's legitimate color scheme.



Image-based scams are more likely to make it through email filters since some services cannot catch suspicious wording in an image. To avoid these scams, always compare the sender's email address to past communications.

Game Time




Can you spot the image-based scam example?



Get Big Deals This Month Only!

Best Buy <bestbuydeals@gmail.com>
To: Sam Johnson

Hi Customer!
We are having big deals!
Scan the QR Code below to access these deals quick!




A

Shop 4K TVs under \$400!

Best Buy <BestBuy@email.bestbuy.com>
To: Sam Johnson

Hi Sam J.



We have fire TVs on sale for under \$400! Check out this 48-hour sale today!

Shop Now

B

HINTS

- Verify the sender's address
- Be wary of unsolicited QR codes
- Check for text that looks stretched or blurry.

Option A is the image-based scam.