SPRING CLEANING

How to improve your digital hygiene

THIS MONTH'S TOPICS:

Out with the old!

Disposing of personal devices securely...

Device Cleaning Checklist

6 ways to refresh your device...

Scam of the Month:

Work Email Scams...

Monthly Mashup:

March updates and review...

Just like many things in life, it is essential that every once in a while, our devices get a deep cleaning. And there's no better time than now!

Digital hygiene refers to the tasks and habits that keep users and their information safe online. But to truly stay safe, keeping devices clean and organized is important.

From backing up data to revisiting old accounts, there are many things to check off the list for improving digital hygiene.

In this month's newsletter, learn what to do with old devices, complete the device cleaning checklist, and identify work email scams. Don't forget to check out the new Monthly Mashup section for some fun jokes and games!

DISPOSING OF PERSONAL DEVICES SECURELY

OUT WITH THE OLD!

Transferring Data

Before throwing out that old device, it is important to have a plan to transfer data. One easy way is to back up everything to a trusted cloud storage solution. You can also use an external hard drive or SSD drive. If you are buying a new device at a credible store, consider bringing the old device and letting an employee complete the transfer for you.

Wiping Devices

Once everything is properly backed up or transferred, it's time to wipe the old device. This protects the security of your data and ensures a smooth transition to the new device. Most devices have a "factory reset" option that wipes all personal data. For more details, research the best way to wipe your specific device.

Selling Devices

In addition to wiping the device, be sure to initiate a factory reset and remove any SIM cards if you plan on selling. Stick to credible websites and look out for common scams that target online sellers. Consider trade-in options at reputable stores, as well.

Work Devices

For the disposal of work devices, it's best to ask your employer for specific company procedures.

Device Cleaning Checklist

- [ ] Unsubscribe from unwanted email lists.
- [ ] Take saved card info off of accounts.
- [ ] Close old email and website accounts.
- [ ] Review social media privacy settings.
- [ ] Set software to automatically update.
- [ ] Stop browsers from storing sensitive data.

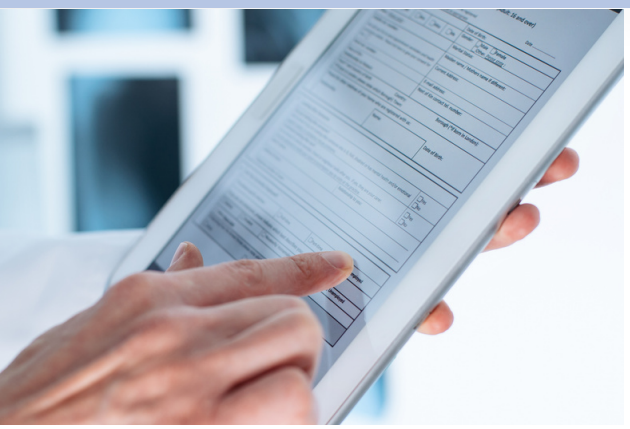
SCAM OF THE MONTH

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

It was a typical day at the office. Connor was checking his inbox when he saw an email from Sarah from HR titled, "Important Dress Code Updates". He was intrigued. *Did something happen with the current dress code? What changes were going to be?*

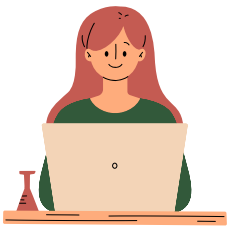
Connor opened the message. It said he must sign a document to show he has read the new policy. There was a link in the message to the new policy and a document to sign. When he clicked the link, he was brought to a website that asked him to make an account. Connor figured it must be a new website HR was using. He entered his phone number, birth date, and other details to sign up.

Once the information was submitted, the screen didn't show the new dress code policy. Frustrated, Connor went over to Sarah's office to ask her about it in person. After talking to Sarah, Connor was shocked to find out she knew nothing about the email.



Did you spot the red flags?

- Connor didn't check the sender's email address. He saw it was "Sarah from HR" and didn't look closer.
- Instead of checking with someone first about the new website, Connor entered all of his personal information.
- Connor let his emotions get the best of him. Cybercriminals often push us to act with "important" messages about topics we expect to see from work.



Always examine the sender's email address closely, even if the name looks familiar. Walk through the SLAM method (sender, links, attachments, message) before acting.

Scammers will create a sense of urgency and call a user to action. Common examples ask a user to sign a document, view an update, or complete an urgent work-related task.

2022 saw an increase in work-related scam emails. Before clicking any links or attachments, check with the person directly to make sure the message is from them. Even if the message appears to be from a website your company uses, it is best to check before clicking any links or entering any information.

THE MONTHLY MASHUP

KEY TAKEAWAYS

It's important to take a step back and examine digital hygiene. By following the device cleaning checklist and the other pointers this month, you can keep your devices clean and your data safe.

JOKE OF THE MONTH

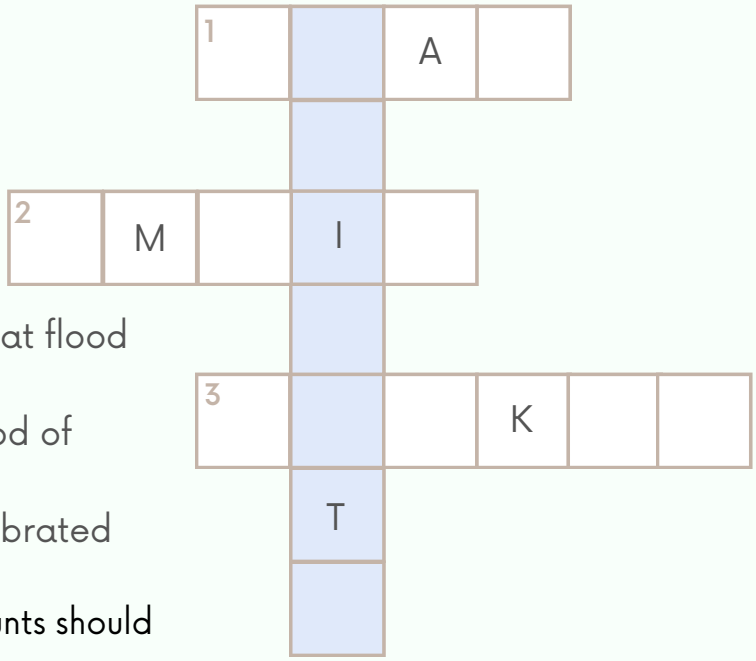
How did the hackers escape?

They ran-som-ware to hide.

MARCH 31ST: WORLD BACKUP DAY

A device could crash, get lost or be stolen, which is why it is so important to secure data by backing it up to the cloud, a hard drive, or a SSD drive.

CYBER CROSSWORD



1. Unwanted messages that flood an inbox.
2. Popular delivery method of phishing messages.
3. The best practice celebrated on March 31st.

Final clue: What all accounts should be set to.