SUSTAINABLE SECURITY

Sustainable security best practices to keep your online world safe

THIS MONTH'S TOPICS:

Cloud Security

How to implement cloud security

3 R's of Password Protection

Reduce, reuse, recycle

Scam of the Month:

Search Engine Scams...

Monthly Mashup:

Updates and review

Earth Day has come and gone, but now is a great time to make sure your cybersecurity habits are sustainable too!

While there are countless ways to stay safe online, if your security practices are not sustainable, they likely will not last. Luckily, there are many habits that are easy to maintain. Taking a few minutes once a week to watch a short training video for example, is an easy habit that takes very little time but greatly improves your online safety posture.

In this month's newsletter, learn some sustainable ways to keep your cloud secure, maintain strong passwords, and safely search the web. Don't forget to check out the new Monthly Mashup section for some fun jokes and games too!

Cloud Security

Over the past few years, there has been an increase in the number of users who utilize cloud storage. While cloud storage typically is a secure way to store data, it is important to know the best practices to implement when it comes to cloud security.

Work Cloud Storage

-Limit cloud access to those who need it.

-Don't access work files on unsecure networks.

-Don't upload work documents to personal cloud storage or share with those who do not have authorized access.

Personal Cloud Storage

-Consider putting additional protections on documents that contain personally identifiable information.

-Use Multi-Factor Authentication on all cloud storage websites.

Cloud Statistics

-94% of all organizations use cloud services.

-The amount of sensitive data shared on the cloud has doubled in the past few years.

-88% of cloud breaches are caused by human error.

Cloud Breach Tactics

-Cybercriminals typically target end users to access the cloud. Avoid public Wi-Fi and follow cybersecurity best practices to avoid a breach.

-Cybercriminals look for vulnerabilities in cloud systems so try to use a cloud service that consistently implements updates and patches.

3 R'S OF PASSWORDS

WHAT ARE THE 3 R'S?

In cybersecurity, reducing, reusing, and recycling does not have the same positive affect that it does for the environment. So when it comes to creating a password, make sure to avoid these three elements.

AVOID THESE 3 R'S:

REDUCE

Make sure you don't reduce passwords to short or simple words. Use at least 11 characters. Consider a passphrase that uses a mix of letters, numbers and symbols.

REUSE

Avoid reusing passwords across accounts. If a breach occurs and a cybercriminal gains access to your credentials, the damage could be multiplied if that same password is used for other accounts, as well.

RECYCLE

Don't recycle old passwords. If a breach occurs, passwords should be changed to something new and different. Instead of changing just a single character, change each password to a completely new passphrase.

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.

Joe was preparing to make a big purchase as a surprise for his wife, so he first checked their bank account balance on their bank's website. Joe typed in the bank name on his search engine and clicked the first search result that came up. The search result included the bank's name and stated it was the official login page.

As the page loaded, Joe noticed that the URL was different than normal and that the lock symbol was missing from the address bar. Before Joe could exit the website, it loaded, and his fears were confirmed.

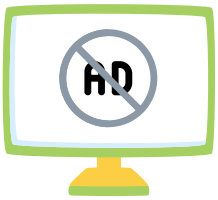
A red pop-up appeared stating, "Your device has been infected with Malware." Joe panicked and clicked out of the website. At first, he was terrified, thinking of all the damage he could have caused. But then, he started thinking of his cybersecurity training. Joe scanned his computer for malware and once it was clean, he changed his bank password and all other passwords that could have been compromised.

Did you spot the red flags?

- Joe didn't check the URL before clicking on the website, he just checked the name which can be modified to mimic real websites.
- Instead of scrolling down past the ads, Joe clicked on the first search result that popped up.
- Joe could have typed in the bank website directly, but he entered the name into the search engine instead.

Type in websites directly and for websites you visit often, bookmark them on your browser to avoid search engine ads.

Avoid ads at the top of search results. Cybercriminals can pay to have their websites posted as ads. Consider using an ad blocker.



Avoid searching for websites on your phone as it is harder to tell if they are secure and easier to accidentally click on an unknown link. If you do click on a malicious link, alert your IT department or someone at your organization.

THE MONTHLY MASHUP

KEY TAKEAWAYS

It takes a realistic balance to make security best practices sustainable. Take the time to complete simple tasks like enabling MFA and using strong passwords to instantly make accounts more secure.

JOKE OF THE MONTH

What is Cyber Cat's favorite meal?

Phish and chips!

MAY 4TH: WORLD PASSWORD DAY

World Password Day is a great day to evaluate passwords. Make sure all passwords are unique. Try using passphrases and multi-factor authentication.

CYBER WORD SEARCH

1. **Cloud**: Remote data storage.
2. **Reuse**: Avoid reusing passwords.
3. **Ads**: Don't click on ads at the top of search results.

F	R	U	G	E	T
W	C	E	B	A	H
C	L	O	U	D	M
J	D	V	F	S	N
T	R	O	P	D	E