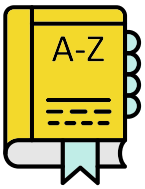
CYBERSECURITY DEFINED

The terms and to-dos for top-notch security

THIS MONTH'S TOPICS:

This month, we're focusing on the building blocks of cybersecurity by defining key terms and highlighting simple actions you can take to strengthen your digital defenses. From understanding the basics of encryption and firewalls, to tackling common threats like NFC (tap-to-pay) scams, this month's newsletter is packed with practical insights.

In this newsletter, you'll find a clear breakdown of cybersecurity concepts, a handy to-do list for securing your accounts, and a spotlight on the latest scams to help you stay one step ahead of cybercriminals.



The National Cybersecurity Alliance's

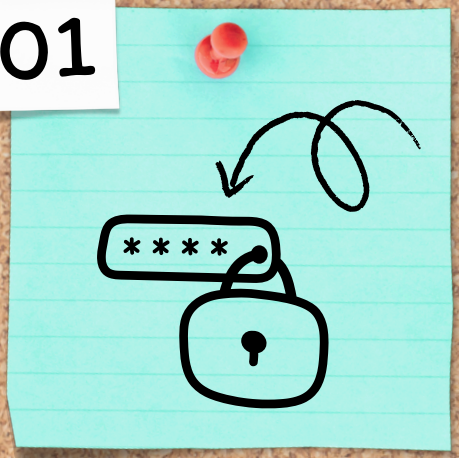
CYBER Definitions

Backup	The process of copying data for recovery purposes in case the original data is lost or corrupted.
Cookies	Pieces of data which detail your browsing history. Used by sites to personalize ads and retain history like cart items. Before a website can track your cookies, they must ask for your consent.
Encryption	A method of scrambling data to make it unreadable. Only someone/something with a decryption key can read the data, keeping information protected.
Firewall	A tool that monitors incoming and outgoing network traffic. It acts as a barrier, allowing trusted data through and blocking harmful connections.
Virus	Harmful programs that can be transmitted to devices in several ways. Viruses are designed to spread themselves, causing havoc in the process.
Zero Trust	A system where no entity is trusted by default, even those inside a network. This framework often leads to more authentication requirements.

Cybersecurity

TO-DO LIST

01



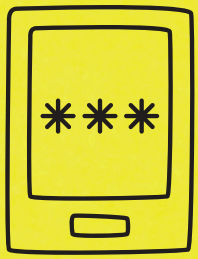
Update Passwords

While passwords no longer need to be updated regularly, they should be updated if a breach has occurred. Use dark web monitoring services and watch for any emails from organizations citing potential breaches of your data.

Use MFA

Multi-factor authentication should be enabled on all accounts where it is offered. Check for MFA enablement under settings or security settings. Many accounts also offer passkeys which can provide additional security.

02



03

Tell a Friend

Take a moment to tell your friends, family, and coworkers about the cybersecurity lessons you've learned. Whether it's sharing a quick takeaway about strong passwords, or helping verify a suspicious link, every lesson can make a difference.

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.

Rachel had just finished a long day of shopping when she received a text notification:
"Fraud alert: Unusual transaction detected. Tap the link to verify your purchases." The link took her to what looked like her bank's official website, asking her to log in to confirm recent NFC transactions. Without hesitation, she entered her username, password, and the one-time code sent to her phone.
Within minutes, her phone buzzed again, but this time it was real banking alerts showing a series of unauthorized NFC transactions draining her account. Confused and panicked, Rachel called her bank, only to find out they never sent that first, original text message.
Rachel had just fallen victim to a scam known as NFC phishing. The fraudulent link had stolen her login credentials, granting the scammers access to her digital wallet. They remotely activated her NFC payments, making high-value purchases before she could even realize what was happening.

Did you spot the red flags?

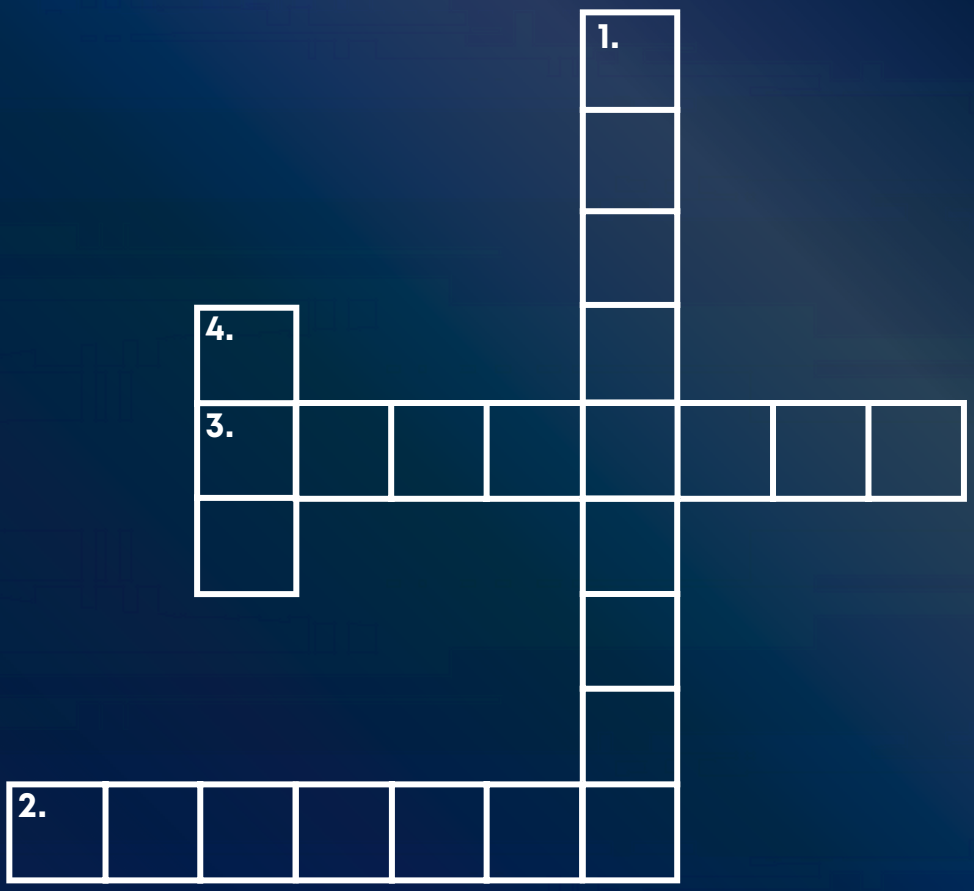
- Rachel should have never clicked on unsolicited texts claiming to be from her bank. She should have gone directly to her bank's official app.
- She should have enabled extra authentication for NFC payments, such as a fingerprint or face recognition, to prevent unauthorized transactions.

In general, enabling notifications for transactions made on your accounts can help keep you aware and mitigate further loss. However, always go through the bank's app, or contact official and trusted channels in order to investigate alerts sent to you via email or text.

Whenever possible, enable multi-factor authentication so that an additional layer of verification is required before a purchase can be made via tap-to-pay methods.

Game Time

Use the clues below for Cyber Crossword!



1. These cyber safeguards should be updated if breached.
2. Pieces of data which detail your browsing history.
3. A barrier that monitors network traffic.
4. An authentication method requiring two forms of verification.

1. Passwords, 2. Cookies, 3. Firewall, 4. MFA/2FA