PROTECTING DIGITAL ACCESS

Why secure authentication is about more than passwords

THIS MONTH'S TOPICS:

Are Strong Passwords Enough?

Add More Layers to Protect Your Accounts

Limit Access, Reduce Risk

The Danger of Overprivileged Access

Security at Your Fingertips

How Biometrics are Changing Authentication

Scam of the Month:

MFA Fatigue Scams

Protecting an account involves more than creating a strong password. Effective security also depends on verifying identities, limiting what each user can access, and recognizing when someone is attempting to get in without permission.

In this month's newsletter, we explore why passwords need additional protection, how excessive permissions increase risk, and how biometric authentication is changing the way we verify identity. We'll also examine an MFA fatigue scam and explain why you should never approve a login request you did not initiate.

ARE STRONG PASSWORDS ENOUGH?

For years, employees have been told that strong passwords are the key to protecting accounts. Long, unique passwords or passphrases still matter, but passwords have an unavoidable weakness: they can be stolen.

Cybercriminals may obtain passwords through phishing, data breaches, malware, or fake login pages. Even a complex password cannot protect an account if an attacker convinces someone to enter it on a fraudulent website. That is why effective account security relies on multiple layers, not a password alone.

A strong password helps protect against:

- Automated password-guessing attacks
- Criminals using common or predictable passwords
- One compromised account exposing other accounts

****

But it cannot stop every threat:

- A phishing site capturing the password
- Malware recording login information
- A reused password appearing in a data breach
- Someone approving a fraudulent login request

****

What Stronger Protection Looks Like: Use a unique passphrase for every account and store it in an approved password manager. Then enable multi-factor authentication, or MFA, whenever it is available. MFA requires an additional form of verification, such as an authenticator app, security key, or biometric check.

Key Takeaway: A strong password should be the beginning of account security—not the end. Combining strong passwords with MFA and careful login habits makes it significantly harder for an attacker to take control.

LIMIT ACCESS, REDUCE RISK

Employees need access to files, systems, and applications to do their jobs, but they do not need access to everything. Overprivileged access occurs when someone has more permissions than their current responsibilities require.

This can happen when access is granted “just in case,” temporary permissions are never removed, or an employee changes roles without having old access revoked. Over time, unnecessary privileges can quietly accumulate.

WHY EXCESSIVE ACCESS CREATES RISK:

A LARGER TARGET FOR ATTACKERS

If an overprivileged account is compromised, the attacker may be able to reach sensitive data or systems that the employee rarely uses.

GREATER CONSEQUENCES FROM MISTAKES

An accidental deletion, incorrect file-sharing setting, or misdirected message can cause more harm when the user has broad permissions.

INCREASED INSIDER RISK

Excessive access gives both careless and malicious insiders more opportunities to view, copy, change, or remove information.

HARDER ACCESS MANAGEMENT

Outdated permissions make it difficult for an organization to know who can access sensitive resources and whether that access is still appropriate.

THE PRINCIPLE OF LEAST PRIVILEGE:

Employees should receive only the access needed to perform their current responsibilities, and only for as long as it is needed. Permissions should be reviewed whenever someone changes roles, completes a temporary project, or leaves the organization.

Security at your FINGERTIPS

Biometric authentication uses a person's physical or behavioral characteristics to help verify their identity. Fingerprint readers and facial recognition are already common on phones, laptops, and workplace systems. Some technologies can also evaluate a person's voice, eyes, or the way they type.

Biometrics can make authentication faster and more convenient because employees do not need to memorize or enter another code. They can also reduce reliance on passwords that may be guessed, reused, or stolen.

Organizations use biometrics because...

Convenience: A fingerprint or facial scan can provide quick access.

Resistance to password theft: Attackers cannot obtain a biometric through ordinary password guessing.

Support for passwordless security: Biometrics can help unlock a device-based passkey without transmitting the biometric itself.

Stronger verification: Biometrics can serve as one component of multi-factor authentication.

Biometrics don't come without risks, though. A biometric is not simply a more advanced password. If a password is exposed, it can be changed. A person cannot replace a fingerprint or face in the same way. Biometric systems must therefore store and process this information securely.

Attackers may also use photographs, recordings, deepfakes, or other techniques to imitate biometric traits. Secure systems use protections such as "liveness detection" to determine whether the person is physically present, but employees should never assume that biometrics make an account invulnerable.

Use Biometrics Wisely:

- Use biometrics only on trusted, organization-approved devices and services.
- Keep devices and biometric software updated.
- Combine biometrics with other safeguards when required.
- Report unexpected authentication prompts or repeated failed scans.
- Never approve access simply because a biometric prompt appears.

SCAM OF THE MONTH: MFA FATIGUE ATTACKS

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

Brian was finishing work when several unexpected login approval notifications appeared on his phone. He denied the first few, assuming someone had entered the wrong information. A few minutes later, he received a call from someone claiming to be from his company's IT department. The caller said a system issue was causing the repeated notifications and asked Brian to approve the next request so they could "fix" his account.

The caller was actually a cybercriminal who had obtained Brian's password and was repeatedly attempting to sign in. The notifications were not an error—they were the final barrier protecting his account. By creating confusion and pretending to offer help, the attacker hoped Brian would eventually approve the request.

DID YOU SPOT THE RED FLAGS?

- An MFA notification appeared even though Brian was not trying to sign in.
- The caller asked Brian to bypass normal caution and approve a request he did not initiate.

HOW TO PROTECT YOURSELF

- Never approve an unexpected MFA request. Deny it and report it through your organization's approved process.
- Verify IT requests independently. Contact your IT team using a trusted phone number or internal channel, not contact info provided by the caller.