# WIZARDS AND WHALES: WHY SOME ROLES ARE BIGGER CYBER TARGETS

In every organization, some people hold more power, more access, or more visibility—and cybercriminals know exactly who they are.

This week, we focus on two types of high-value targets:

- Wizards: Your IT staff, engineers, and developers, the people who run the tech behind the scenes.
- Whales: Executives, directors, and public-facing leaders, the decision-makers and brand voices.

## Why These Roles Matter to Attackers

- Wizards hold admin powers, like unlocking doors in the digital world. If their accounts get hacked, attackers can do serious damage fast.
- Whales are high-profile and often publicly listed, making them easier to impersonate or trick with phishing and social engineering.

Cybercriminals go after these roles because one slip-up can lead to massive payouts—data breaches, financial fraud, or worse.

## A Real Example

In 2020, hackers tricked Twitter employees (the wizards) into giving up internal access. From there, they hijacked the accounts of VIPs like Elon Musk and Barack Obama (the whales) and launched a bitcoin scam.
Source: U.S. Department of Justice

## What You Can Do

Even if you're not a wizard or a whale, you still play a key role in keeping them safe:

- Be skeptical of unusual emails or messages from leadership.
- Don't share credentials or reset passwords without following proper processes.
- Report suspicious behavior especially if it involves high-level users or system access.

## Final Thought

Security isn't just a tech issue; it's a people issue. Everyone needs to work together to protect the people with the most access and the biggest bullseyes on their backs.

Explore CyberEd.io's awareness training built for teams of all sizes, including guidance for supporting privileged users and protecting high-profile roles.

# WIZARDS AND WHALES: PRIVILEGE, PROFILE, AND THE CYBERSECURITY PRESSURE POINT

This week, we zero in on the two most strategically important attack surfaces in your organization: privileged users (wizards) and high-profile individuals (whales).

- Wizards: Admins, engineers, and developers with backend access and powerful credentials.
- Whales: Executives, board members, and public-facing figures with financial authority, reputational influence, and often, poor security hygiene.

## Why They're Prime Targets

- Access + Visibility = Amplified Risk
- Wizard risks: Lateral movement, escalation of privilege, shadow tooling, misconfigured automation.
- Whale risks: Business email compromise, deepfake fraud, impersonation attacks, and delegation chains with poor visibility.

Attackers exploit both groups through tailored phishing, compromised endpoints, and social engineering, often chaining the two (e.g., compromise a wizard → target a whale).

## Real-World Case: Twitter 2020

A coordinated social engineering attack targeted internal staff (wizards) to gain access to admin tools. The attackers then took over whale accounts like @elonmusk and @apple, publishing scam messages and damaging public trust.
Source: DOJ Report

## Mitigation Strategies

For Wizards:

- Enforce least privilege access and time-based elevation
- Require MFA with hardware tokens
- Monitor and alert on out-of-band activity and internal tool usage
- Conduct regular privilege audits, particularly across CI/CD pipelines, IaC, and DevOps tools

For Whales:

- Deploy VIP-tier protection protocols (e.g., hardened mobile devices, zero-trust authentication, real-time threat monitoring)
- Limit social exposure and reduce public metadata (e.g., travel, org charts, job titles)
- Train executive assistants and support staff on targeted phishing and vendor fraud patterns

For General Users:

- Train general users on what to look for and be specific. Give them examples that relate to their roles.
- Develop open communication policies. Make it easy for them to report an issue or ask for verification, without fear of penalty or admonishment.

## Security Is a Team Sport

Your SOC might be stellar, but if privilege isn't properly gated, or if your CEO clicks the wrong link, your incident response playbook is already on fire.

Dig deeper with CyberEd.io's role-based training, including expert-level content on securing privileged identities, high-profile execs, and hybrid cloud attack surfaces.