

# Research showing that retired professors themselves are not a cybersecurity threat

ChatGPT 14.03.2026

Some universities are terminating university email accounts for professors upon retirement due to "cybersecurity risks". Instead of closing just unused university email accounts of retired professors, the university is deleting the accounts of all retired professors due to "increased cybersecurity exposure". It is important to keep in mind that a retired professor is not just "one of the former employees".

There is very little research showing that retired professors themselves are a cybersecurity threat. Most cybersecurity literature focuses on accounts that remain active after employment ends, not on retirees as a group behaving maliciously. In fact, several policy papers argue the opposite—that removing retired professors' email access is often not evidence-based.

Below are the closest research findings related specifically to universities and retired faculty accounts.

## 1. *Studies focus on "dormant accounts," not retirees*

Cybersecurity research on universities consistently identifies email accounts as a major attack vector, because institutional email often grants access to many internal services.

A study of academic collaboration networks found that email systems are central nodes of institutional communication, meaning that compromising one account can expose many other systems and contacts.

Because of this, security policies often target inactive or rarely used accounts. These may include:

- former staff
- retired professors
- alumni accounts
- inactive student accounts

The risk comes from unused identities, not from retirees' behavior.

## 2. *University policies rarely cite retirees specifically*

Policy debates among retired academics note that universities often cancel email accounts automatically at retirement, but the reasons are administrative rather than evidence of risk.

A policy statement from the Professors Emeriti Network notes that universities differ widely: some keep accounts for retired professors while others terminate them immediately, even though emeritus professors often retain full access.

The same statement argues that removing accounts can harm collaboration and continued research participation by retired faculty.

### *3. No studies showing retired professors cause breaches*

In the academic cybersecurity literature:

There are no peer-reviewed studies demonstrating that retired professors themselves cause cyber incidents.

The risk models instead address identity lifecycle management (creating and deleting accounts).

The concern is usually unused accounts becoming compromised by external hackers.

### *4. Why IT departments sometimes include retirees anyway*

From a security engineering perspective, policies treat all accounts the same:

- Active staff → necessary accounts
- Anyone else → potential unnecessary identity

Cybersecurity frameworks such as role-based access control research emphasize limiting accounts only to users with active roles in the organization.

So, universities may remove retired professors' accounts simply because their role ended, even if the individual is trustworthy.

### *Summary*

Research evidence shows:

- Email accounts at universities are a major security entry point.
- Dormant accounts are considered risky.

However, there is no research showing retired professors themselves are a cybersecurity threat.

Most policies deleting their accounts are based on general identity-management rules, not specific evidence about retirees.

### **Many major universities actually allow retired professors to keep their email accounts, which suggests the cybersecurity justification is debate**

Policies at several major universities show that retired or emeritus professors can retain university email accounts, though usually under certain conditions. This variation is exactly why the cybersecurity argument is debated rather than universally accepted. Here are concrete examples.

#### *1. University of Cambridge*

Cambridge explicitly allows some retirees to keep their institutional email accounts.

- Individuals with emeritus or honorary titles remain eligible for a university email account.
- Retired staff can retain accounts if they continue contributing to the university's mission (research collaboration, seminars, etc.).

- The official email policy states that emeritus and honorary members are eligible to hold a @cam.ac.uk address.

This shows that Cambridge considers the continued academic role of retirees more important than automatically deleting accounts.

## 2. University of Oxford

Oxford also allows some retirees to keep email access.

- Retired staff may retain email and IT access if they apply for a retiree card.
- Access depends on the retiree's affiliation status and whether they remain connected to the university.

This indicates a case-by-case approach rather than automatic deletion.

## 3. Other universities with emeritus email access

Many universities allow emeritus faculty to retain email indefinitely, because they:

- continue publishing research
- supervise graduate students
- collaborate internationally

For example, policies at institutions like Colgate University explicitly state that emeritus faculty may retain their university email accounts for ongoing scholarly work.

## Why policies differ

Universities tend to fall into two broad models:

### *Model A — retain accounts*

Common for emeritus professors.

Reasons:

- retired professors still publish under university affiliation
- their email appears in journal articles
- they collaborate with active faculty

### **Model B — delete accounts**

Some universities now close them because:

- identity-management policies treat any non-employee account as extra risk
- email accounts often provide access to many internal systems

## Key takeaway

The cybersecurity argument is not universally applied:

- Some universities keep retired professors' accounts with restrictions.
- Others remove them automatically to reduce unused identities.

Because both approaches exist at leading universities, the policy choice is administrative and risk-management based, not the result of clear research showing that retired professors themselves are a cybersecurity threat.

# Google AI Mode

Research indicates that while retired professors and older adults generally are frequently targeted by cybercriminals, they are not inherently a higher risk to institutional cybersecurity systems themselves, and in many contexts, they demonstrate comparable or even superior caution compared to younger, more active users.

## 1. Counter-Stereotyping Findings

**High Resilience:** Contrary to the belief that older adults are the highest-risk group, studies on "knowledge worker" cybersecurity behaviors found that older employees often demonstrate high resilience, while younger, more "flexible" users (such as students or temporary staff) may actually pose a higher risk due to more lenient security practices.

**High Caution Levels:** Research suggests that older users often display more "online guardianship behaviors," such as using antivirus software, and are often more cautious or suspicious of digital interactions than younger counterparts.

**Equal Phishing Suspicion:** Studies analyzing phishing detection show that older adults (65+) do not necessarily have lower accuracy in identifying phishing emails than younger adults, though they may take longer to classify them.

## 2. Context of Risk (Targeted vs. Threatening)

Research distinguishes between being a victim of crime and being a threat to an organization:

**Targeted as Victims:** Retirees are frequently targeted for phishing, romance scams, and financial fraud because they are viewed as vulnerable.

**Not Actively Malicious:** There is no evidence suggesting retired professors actively threaten institutional data security, but rather, their accounts may become "orphaned" if not managed, which is a structural IT issue, not a behavioral issue.

## 3. Mitigating Factors

**Education Levels:** Research indicates that "years of education" acts as a protective factor against phishing susceptibility, which is highly relevant to retired professors.

**Social Support:** Retired academics often have strong social and professional networks, reducing the isolation that often leads to increased susceptibility to scams.

## Key Takeaway

The research argues for moving away from ageist stereotypes that categorize all retirees as a security risk. Instead of viewing retired professors as a threat, research suggests implementing tailored, human-centered security awareness training to help them manage their online safety, as they are a diverse group with varied skill sets.