

PROTECTING YOUR IDENTITY

University of Miami Ethics Programs

WHY WORRY ABOUT YOUR IDENTITY?

- **Workplace security** – Identity security is the cornerstone of protecting not just an organization’s information, but its physical, financial and human resources as well.
- **Your own security** – Learning to protect your identity at work can protect you from personal identity theft, an increasingly common crime.

The goal of a security system is to let the right people in, and keep the wrong people out. That’s true when we are talking about physical spaces like building, and virtual spaces like the files on a computer. Security systems must also make sure that the right people, once let in, do only the right kinds of things. Identity security is critical to both of these.

SUGGESTIONS FOR PROTECTING YOUR IDENTITY

- **Preserve physical security** – Controlling physical access is critical. Keep an eye out for persons who appear to be in the wrong place. Don’t be afraid to politely challenge a stranger for ID.
- **Protect things that control physical access** – ID badges, card keys, conventional (metal) keys, lock codes and anything else that controls physical access must be kept secure.
- **Be aware of the dangers of the virtual world** – It’s much more difficult to identify persons that exist only as telephone voice, on a fax, in an email or a postal letter. Extra care is always required.
- **Know who you’re dealing with** – Confirm the other party’s identity before you exchange any sensitive information. Take the time to ask needed questions.
- **Protect personal data** – Aside from preserving privacy, this is critical to protecting identity. Personal data like SSNs, birth dates, and parents’ names are often used to establish identity. Be careful about how you store such data, and about how you dispose of copies of it.
- **Protect passwords especially** – Many information systems use password to control access. That makes it particularly critical to pick good passwords and protect them appropriately.
- **Protect access “tokens”** – Smart cards and USB keys are increasingly used to control computer system access. For obvious reasons, these need to be protected too.
- **Biometrics are coming** – Fingerprints, retinal scans and other body measurements will be used to control access in the future. For now, you’ll have to remember passwords and keep track of tokens.
- **Access controls set limits** – Most information systems restrict what particular users can do, using access controls. If you need additional access privileges, make a formal request. Don’t borrow someone else’s ID, even if it’s just “temporary.”

- **Audit trails record activity** – Be aware that computer systems record each user’s activities, sometimes in great detail. This is another reason to protect your identity, since anything done with your stolen ID will appear to have been done by you.
- **Use activity data yourself** – Information about when you last logged in or changed a file can help you discover if someone else has “borrowed” your identity.
- **Security mistakes happen** – Be patient if identity security measures lock you out sometimes. It’s part of the price of security.
- **Security inconvenience happens** – Even when everything goes right, security procedures require time and inconvenience. This is part of the price of security too.

► *Questions and comments about this document are welcome. Send email to ethics@miami.edu.*