

Everyday Passwords

This memo catalogues all of the passwords I use regularly and the restrictions on each. I will then give my recommendations for password policy.

I put my passwords in the following four categories: work, finance and shopping, school, and home. The categories are based on what area of my life I use them. The passwords in each category share some similar traits. My work based passwords were generally the most restrictive. Almost all of my web based passwords used my email address as the ID. My passwords I used at home were the least secure.

My Passwords

	Password	Min Length	ID	Content Requirements	Expires	Reuse Restrict.
Work	Active Directory Password	8 Char	assigned username	upper and lower case chars, #s or symbols	3 months	cant use last 10 passwd.
	VPN Certificate	8 Char	assigned username	upper and lower case chars, #s or symbols	never	none
	Telecom Equip Admin.	6 Char	assigned username	none	never	none
	Web Proxies Admin	8 Char	shared username	none	never	none
	Wireless LAN Admin	None	shared username	none	never	none
	IBM Support Site	6 Char	email			
	Cisco TAC Support Site	5 Char	self selected username	none	never	none
	Network Appliance Support Site	6 Char	email	none	never	none
	Instant Messaging	6 Char	assigned username	none	never	none
	Document Sharing Site	1 Char	assigned username	none	never	none
	Foundstone Security Scans	Assigned	assigned username	characters, symbols, numbers (assigned)		
Finance & Shopping	Brokerage	6 Num	SSN	numbers	never	none
	Online Bank	6 Num	assigned account #	numbers	never	none
	BarnesandNoble.com	3 Char	email	none	never	none
	Ticketmaster.com	5 Char	email	none	never	none
	Celtics Web Site	5 Char	assigned account #	none	never	none
School	Bentley.edu alumni	1 Char	self selected username	none	never	none
	MyNeu	6 Char	assigned username	none	never	none
Home	Home PC	none	self selected username	none	never	none
	Home Laptop	none	self selected username	none	never	none

Password Development Recommendations:

Software developers must maintain a balance when creating password restrictions. If they are too complex, people will have difficulty remembering them. This will cause more support calls. Another risk of complex passwords is that people will be tempted to write them down.

On the other hand, if a password has little or no restrictions, people will tend to pick common passwords. Then dictionary attacks become more effective on the password. The password should have at least enough restrictions to avoid dictionary attacks.

Developers should consider the impact if the password is compromised. If the impact to a person or the organization is very high, then complex passwords should be used. Rotating passwords should also be considered. If the impact is low, it is appropriate to have less complex passwords.

The selection of a user ID is also a key factor in how safe a password is. Many passwords use the person's email address for the ID. This is convenient since it allows developers to contact people and it ensures a unique ID. The risk to this is that an attacker might know a person's email or could guess it. And if they have compromised one password, chances are that the person has used the same password on other sites with the email address as the ID.

Another risk to email address IDs is if a person's email account is compromised. An attacker could log on to a site and have the password reset. The password is then usually sent to the person's email address. The attacker could then see the password. Developers should avoid using email addresses as IDs unless the impact of being compromised is very low.