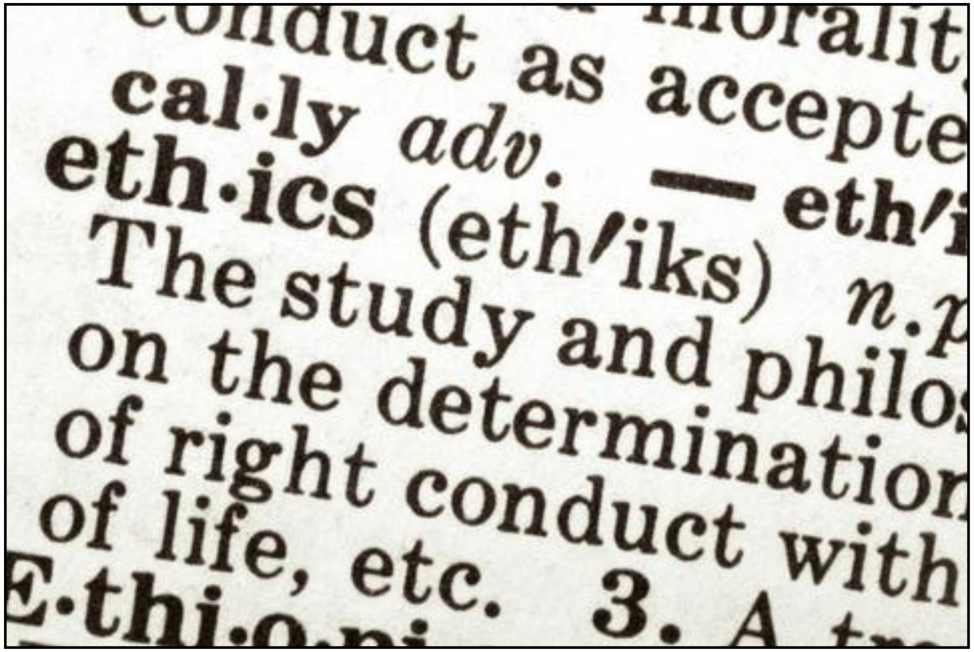
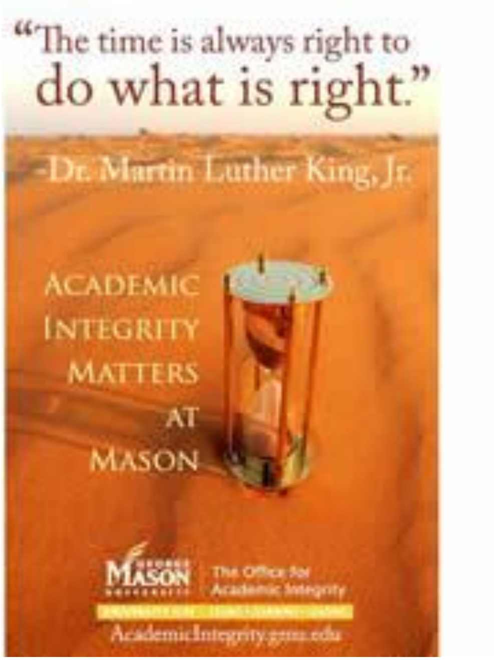
Data Ethics in an Information Society (from the course **CDS 151**)

I.T. Ethics in Theory and Practice



moralit
onduct as accepte
cal·ly *adv.* — eth′i
eth·ics (eth′iks) *n.p*
The study and philos
on the determinatio
of right conduct with
of life, etc. 3. A tr
E·thi·o·pi


"The time is always right to do what is right."
-Dr. Martin Luther King, Jr.
ACADEMIC INTEGRITY MATTERS AT MASON
GEORGE MASON UNIVERSITY
The Office for Academic Integrity
AcademicIntegrity.gmu.edu

Outline

- Mason’s Definition of I.T. Ethics
- The Rules of I.T. Ethics
- I.T. Ethics in Practice: the 2+2 perspective

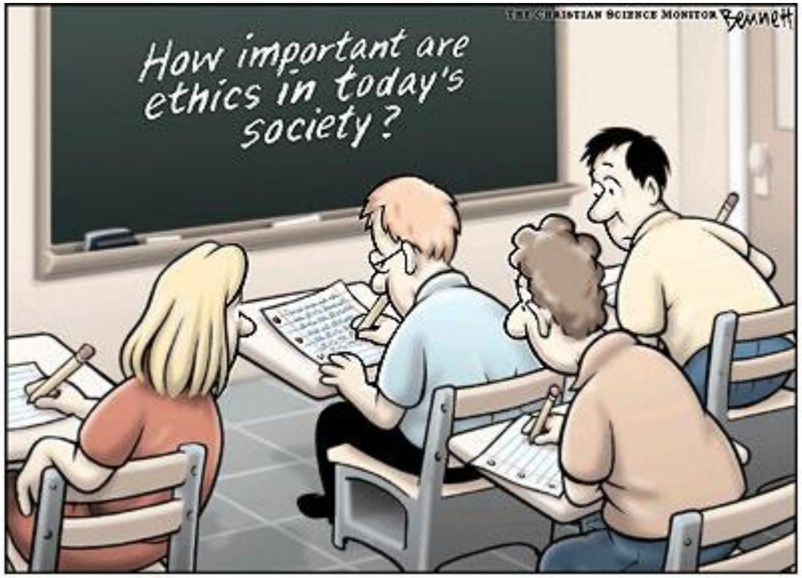
How does Mason define I.T. Ethics?

- Mason's I.T. Ethics Gen Ed requirements:
  - Students will understand many of the key ethical, legal and social issues related to information technology and how to interpret and comply with ethical principles, laws, regulations, and institutional policies.
  - Students will understand the essential issues related to information security, how to take precautions and use techniques and tools to defend against computer crimes.

Outline

- Mason's Definition of I.T. Ethics
- The Rules of I.T. Ethics
- I.T. Ethics in Practice: the 2+2 perspective

Got Ethics?


THE CHRISTIAN SCIENCE MONITOR
Bennett
How important are ethics in today's society?

Intro to Ethics

got ethics?

Ethics

What is Ethics?

- It is the set of well established principles of right and wrong.
- **It is doing the right thing, even when nobody knows.**

How do you know what is the right thing to do?

- If ethics is “doing the right thing, even when nobody is watching”, then how do you know what is the right thing?
- Fortunately, we have guidance on this.
- In fact, we have 4 levels of guidance:
  - **Principles**
  - **Policies**
  - **Regulations**
  - **Laws**
- We will discuss these in detail.

Principles, Policies, Regulations, Laws

- The 4 levels of Ethical Guidance :
  - Principles
  - Policies
  - Regulations
  - Laws
- They each carry a different (and increasing) burden of responsibility and enforcement.

Principles, Policies, Regulations, Laws

- The 4 levels of Ethical Guidance :
  - **Principles** – these are fundamental truths, doctrines, or motivating forces. These are often overwhelmingly obvious guidelines for proper behavior. For example:
    - Treat other persons with respect.
    - Do no harm.
    - Act with justice.
    - Show no partiality (treat each person fairly).
    - Do not invade or compromise another person’s privacy.
    - The Honor Code
  - Policies
  - Regulations
  - Laws

Principles, Policies, Regulations, Laws

- The 4 levels of Ethical Guidance :
  - Principles
  - **Policies** – these are agreed-upon operational guidelines and procedures (specified courses of action) for organizations, to guide decisions and actions with regard to principles and acceptable behavior. For example:
    - Computer AUP (Acceptable Use Policy)
    - Honor Code Plagiarism Policy
    - Sexual Harassment (can also have Regulation or Law status)
    - Smoking policy ("take it outside")
    - Cell phone use policy during class ("take it outside")
  - Regulations
  - Laws

Principles, Policies, Regulations, Laws

- The 4 levels of Ethical Guidance :
  - Principles
  - Policies
  - **Regulations** – these are rules and restrictions that specify acceptable behaviors or outcomes, consistent with ethical principles and institutional policies. Examples:
    - Plagiarism regulations (you can be expelled from the University, but you are not likely to be put in jail)
    - Safety regulations (you can be reprimanded or fired for not wearing safety goggles in a chem lab or a hard hat at a construction site)
    - Health regulations (restaurants can be closed for violating no-smoking policy)
  - Laws

Principles, Policies, Regulations, Laws

- The 4 levels of Ethical Guidance :
  - Principles
  - Policies
  - Regulations
  - **Laws** – these are regulations that are enacted by governments – they are enforceable by the courts and the legal system – you can be fined, sued, or incarcerated for violation of laws. For example:
    - Lying under oath (Perjury)
    - Downloading and viewing child pornography on your computer (even on your home computer)
    - Violations of copyright and intellectual property laws
    - Scamming other people out of their money
    - Identity theft

What about **I.T.** Ethics?

- Hackers, Phishers, Identity Thieves, …
- They all use some form of inducement, trickery, deflection, fallacy-based reasoning, false inference, confounding factors, or "lying with statistics" to get you to buy into their scam.
- You can be an unwilling participant if not careful.
- There are usually consequences caused by improper uses of information technology (I.T.):
  - Ethical – *"I have to live with my own conscience."*
  - Social – *"I have to live with my family and friends."*
  - Legal – *"I have to live in a society based on law."*

Some Examples of Ethics Policies

- University Code of Ethics
- University Honor Code
- Plagiarism and the Internet
- I.T. Policies
  - Data Stewardship
  - Responsible Use of Computing
  - Electronic Information Environment
- Policies are part of the 4 levels of Ethical Guidance:
  - Principles
  - Policies
  - Regulations
  - Laws

Some examples of ethics policies: (1) University Code of Ethics

https://docushare.gmu.edu/dsweb/Get/Document-48331/Code%20of%20Ethics%20Approved%2012.1.10.pdf

Here are some sample excerpts from the document:

- “We perform our public responsibilities, services and activities ethically, competently, efficiently and honestly, in keeping with University policy and applicable law.”
- “We do not accept any favor, loan, service, business or professional opportunity from anyone knowing that it is offered in order to improperly influence the performance of our public duties.”
- “We preserve and respect the confidentiality of University records, including individual and student records.”
- “We are committed to the principles of federal and state law guaranteeing equal opportunity and nondiscrimination with respect to University services, programs, activities and employment.”
- “We respect the rights and opinions of all people.”
- “We do not condone dishonesty in any form by anyone.”

Some examples of ethics policies: (2a) University Honor Code

http://oai.gmu.edu/honor-code/masons-honor-code/ or http://oai.gmu.edu/

Here are some aspects of the Mason honor code:

- "All members of the University community commit to not **cheat, steal, plagiarize,** or **lie** in matters related to your academic work…
- … To promote a stronger sense of mutual responsibility, respect, trust, and fairness among all members of George Mason University, and with the desire for greater academic and personal achievement."
- There are formal procedures for violations:

http://oai.gmu.edu/honor-code/adjudication-process/

- You have rights (including the right of appeal): http://oai.gmu.edu/students/student-rights/
- Specific rules govern plagiarism = "Intellectual Robbery" http://mason.gmu.edu/~montecin/plagiarism.htm
  - Plagiarism consists of either: (a) "using the exact words, opinions, or factual information from another person without giving that person credit; or (b) borrowing

Some examples of ethics policies: (2b) Plagiarism and the Internet

http://mason.gmu.edu/~montecin/plagiarism.htm

- Copyright rules apply to users of the Internet who cite from Internet sources.
- Information and graphics accessed electronically must also be cited, giving credit to the sources.
- Intellectual Property Law is as serious as Real Property Law.
- Putting someone else's Internet material on your web page is stealing intellectual property.
- The University uses plagiarism-detection software to measure student compliance. For example: **TurnItIn** or **SafeAssign**
  - These companies maintain databases and links to many(!) millions of papers, documents, websites, student reports (e.g., every paper that I have submitted from my students from all past years is now included in the database search).
  - Violations can lead to expulsion from the University.
  - Don't even think about doing it.
  - Even unintentional plagiarism provides a valuable lesson: give proper citations!
  - Reference: http://doit.gmu.edu/studentSection.asp?page=safeassign

Some examples of ethics policies: (3a) I.T. Policies and Ethical Guidelines

http://itu.gmu.edu/policies/index.cfm

- Policies cover many aspects of Information Technology:
  - Data stewardship
  - Internet access
  - Responsible use of computing
  - Telephone and other telecommunications
  - Wireless networking
- Data Stewardship Policy
  - Governs the privacy, security, confidentiality, and governance of university data, especially highly sensitive data
- Internet Access Policy
  - Requires that all computers that need a publicly addressable Internet address be registered with the ITU (http://itu.gmu.edu/)
- Responsible Use of Computing (i.e., **AUP** = **A**cceptable **U**se **P**olicy)
  - This specifies what you should not do and what you must not do with the organization’s computers and computer resources
  - http://universitypolicy.gmu.edu/policies/responsible-use-of-computing/
  - … continued on the next 3 slides …

Some examples of ethics policies: (3b) Responsible Use of Computing, part 1

http://itu.gmu.edu/policies/index.cfm

- Rule #1: Use Mason Computing Resources consistent with the following intended purposes:
  - educational, research, and administrative purposes of Mason
  - uses that are indirectly related to Mason purposes that have an educational or research benefit, such as news reading, web browsing, chat sessions, and personal communications
- Rule #2: Do not use computer accounts for illegitimate purposes.
  - may not use Mason's computing resources for recreation or entertainment
  - may not conduct any of the following FORBIDDEN ACTIVITIES:
    - Selling access to Mason's computing resources;
    - Engaging in commercial activity not sanctioned by Mason;
    - Intentionally denying or interfering with any network resources;
    - Using or accessing any Mason computing resource, or reading or modifying files, without proper authorization;
    - Using the technology to in any way misrepresent or impersonate someone else;
    - Sending chain letters;
    - Violating copyright laws and licenses;
    - Violating federal or state law, or university policy.
- Rule #3: Honor the privacy of other users.

Some examples of ethics policies: (3c) Responsible Use of Computing, part 2

http://itu.gmu.edu/policies/index.cfm

- Rule #4: Do not use any account except the one you have been authorized to use.
- Rule #5: Do not use Mason's computing resources to violate other policies or laws. For example:
  - Using Mason's computing resources to violate harassment laws or policies. Various types of harassment, including sexual or racial, are proscribed by Mason policies.
  - Using Mason's computing resources to violate the Honor Code.
  - Extending the Mason network without explicit permission from ITU Network Engineering. The unauthorized use of routers, switches, modems and other devices can impact the security and stability of the network.
  - Running vulnerability scans on systems are considered hostile. If required for academic reasons, written permission from the system owner is required.
  - Using Mason's computing resources to transmit, store, display, download, print or intentionally receive obscene material, or to distribute pornographic material. All users of Mason computing resources are subject to all federal and state obscenity laws. State employees should also be aware of state laws prohibiting the use of state equipment to access, store, print or download sexually explicit material.

Some examples of ethics policies: (3d) Electronic Information Environment

- Personal e-mail, electronic files maintained on Mason equipment, and personal web sites are part of a unique electronic information environment.
  - This environment creates unique privacy issues that involve federal and state laws as well as Mason policies.
- **Mason reserves the right to inspect user files and communications for all lawful purposes**, to include investigating allegations of illegal activity, violations of Mason policies, or to protect the integrity and security of network systems.
- **Web pages:** Mason will investigate all complaints involving personal web sites and will remove or block material or links to material that violate federal or state law or university policy.
- There are procedures and processes for handling violations and for ensuring compliance:

  http://universitypolicy.gmu.edu/policies/responsible-use-of-computing/#compliance

I.T. Ethics – outcomes & benefits

- There are usually **consequences** caused by **improper** uses of information technology (I.T.):
  - Ethical – *“I have to live with my own conscience.”*
  - Social – *“I have to live with my family and friends.”*
  - Legal – *“I have to live in a society based on law.”*

- Conversely, there are usually **benefits** accrued by **proper** uses of information technology (I.T.):
  - Ethical – *“I am at peace with myself.”*
  - Social – *“I am at peace with my family and friends.”*
  - Legal – *“I am at peace with society and law enforcement officials.”*

Outline

- Mason’s Definition of I.T. Ethics
- The Rules of I.T. Ethics
- I.T. Ethics in Practice: the 2+2 perspective

I.T. Ethics (the “2+2 perspective”)

1. **The good guys**
   - Things that we do (but SHOULDN’T)
   - Things that we don’t do (but SHOULD)

2. **The bad guys**
   - Things that they do in a passive mode
   - Things that they do in an active mode

Reference: http://www.auburn.edu/~fordfn1/aces5770.html

Remember: PII = Personally Identifiable Information

Things That We Do (but shouldn’t)...

- Things that we **do** (accidentally or intentionally):
  - Choose weak passwords (e.g., dictionary word)
  - Share account access information! (unbelievable, but true!)
  - Reveal “Too Much Information” (TMI)
  - Improperly disclose PII (maybe even unauthorized!)
  - Download illegally ➔ **Intellectual property theft**
  - Pirate software ➔ **Intellectual property theft**
  - Visit “questionable” web sites ➔ **Against computer AUP****
  - Transfer sensitive information without securing it first

** **AUP** = **A**cceptable **U**se **P**olicy (http://universitypolicy.gmu.edu/policies/responsible-use-of-computing/)

Things That We Don’t Do (but should)…

- Things that we **<u>don’t do</u>** (or **forget to do**):
  - Choose **<u>and</u>** use strong passwords (**$troNGPa&&w!RD**)
  - Choose **<u>and</u>** use hard-to-guess security pass phrases
  - Encrypt sensitive information to secure it
  - Install and update anti-virus and anti-spam software
  - Use a VPN (Virtual Private Network, if available); use a software-based firewall (Windows, Symantec, etc.)

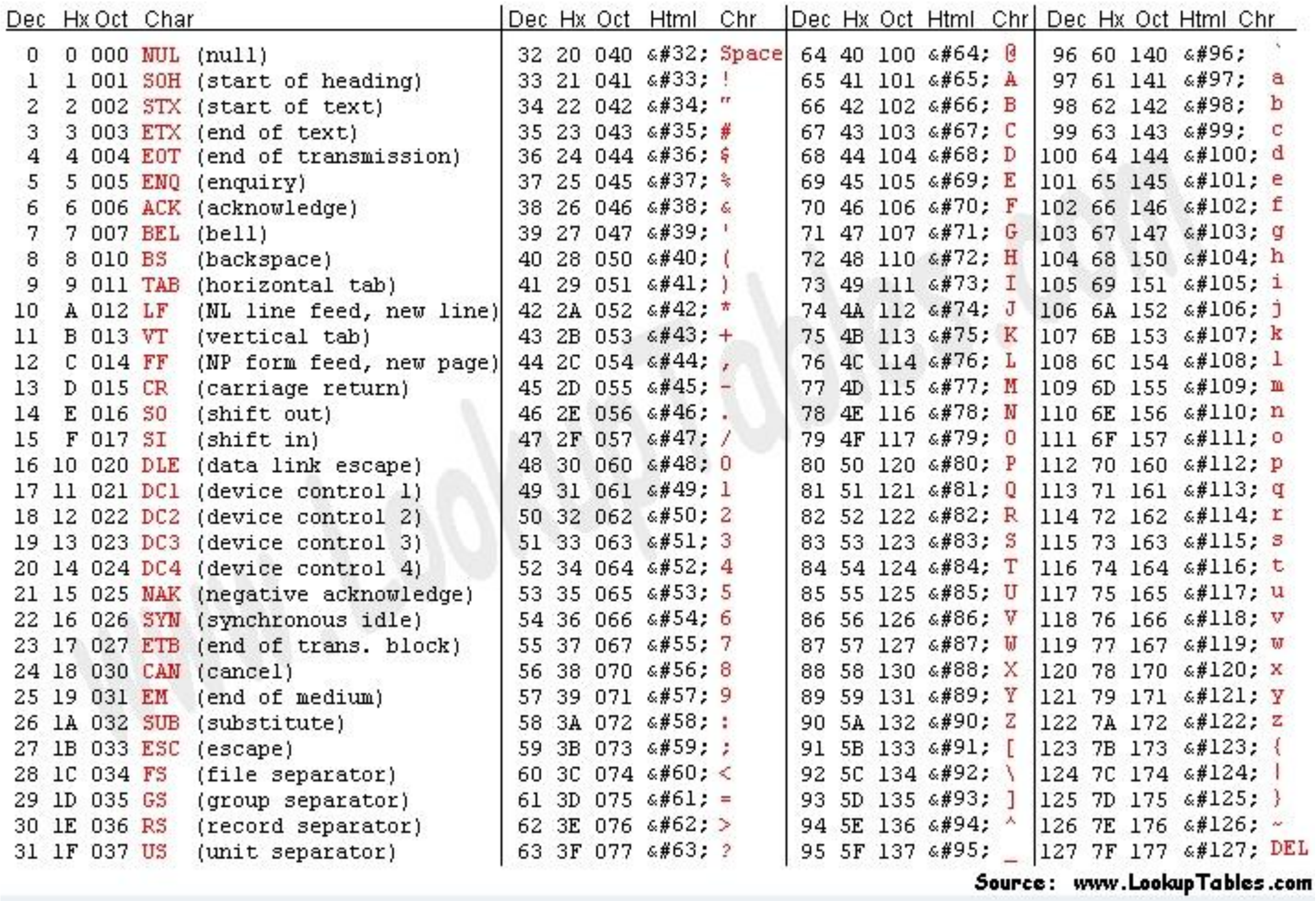
What about Passwords?

- **A STRONG PASSWORD IS YOUR FIRST (AND BEST) DEFENSE AGAINST MALICIOUS INTENT**.
- So let’s take some time to review strong passwords.
- In particular, what makes them “strong”, and why?
- Do strong passwords ***REALLY*** matter, anyway?

The Mathematics of Strong Passwords

- Assume a 5-ASCII character password
  - Each ASCII character is represented by 8 bits, so there are 256 ASCII characters to choose from:
  - 00000000, 00000001, 00000010, 00000011, …, 11111111
- How many passwords could you generate with these 5 ASCII characters? (256 x 256 x 256 x 256 x 256)
- Yep! 256^5 = 1,099,511,627,776 possible passwords!
  - That is over one trillion possibilities!

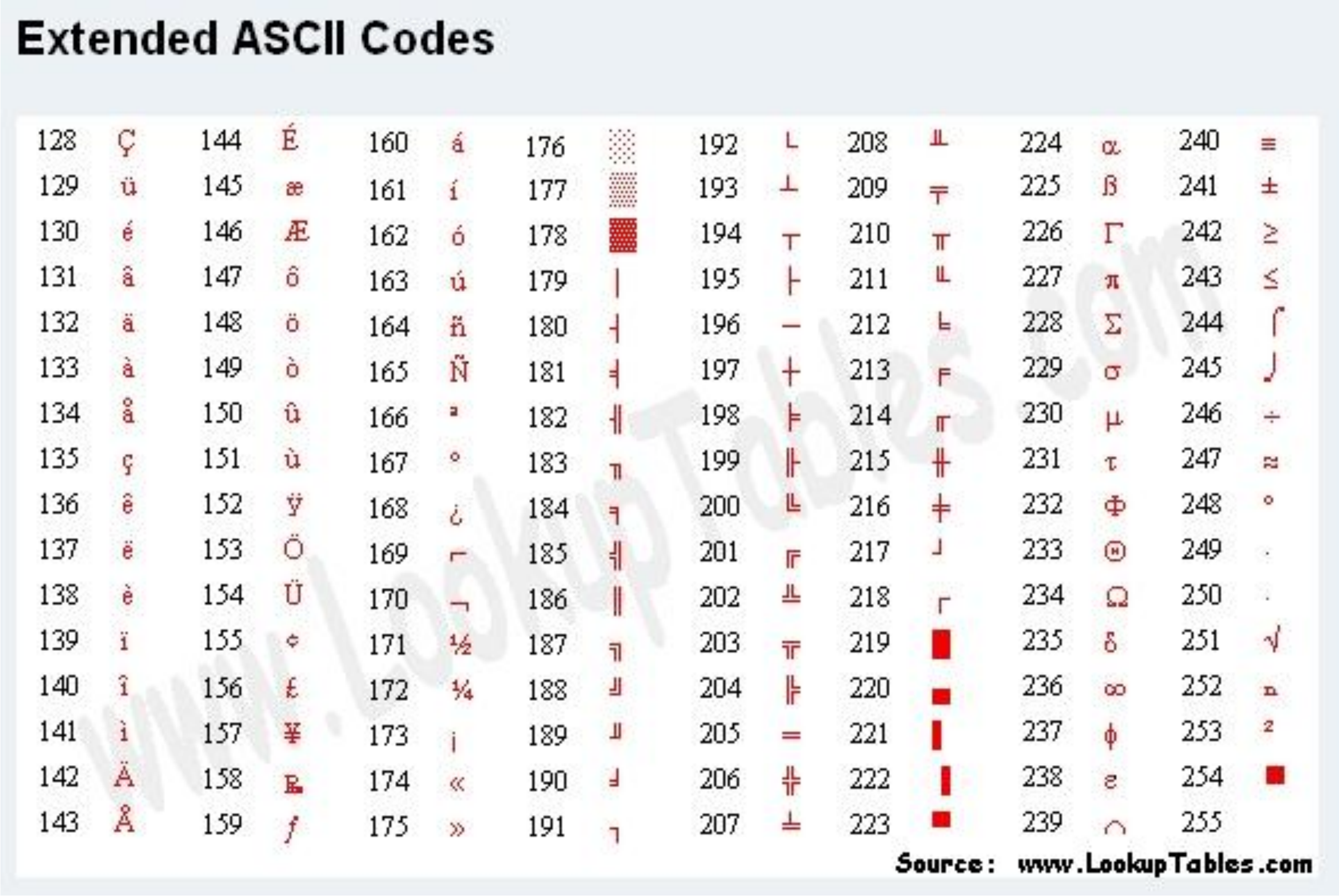
The Mathematics of Strong Passwords



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT (end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ (enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK (acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL (bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS (backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB (horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF (NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT (vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF (NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR (carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO (shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI (shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE (data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1 (device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2 (device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3 (device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4 (device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK (negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN (synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB (end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN (cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM (end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB (substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

The Mathematics of Strong Passwords



Extended ASCII Codes

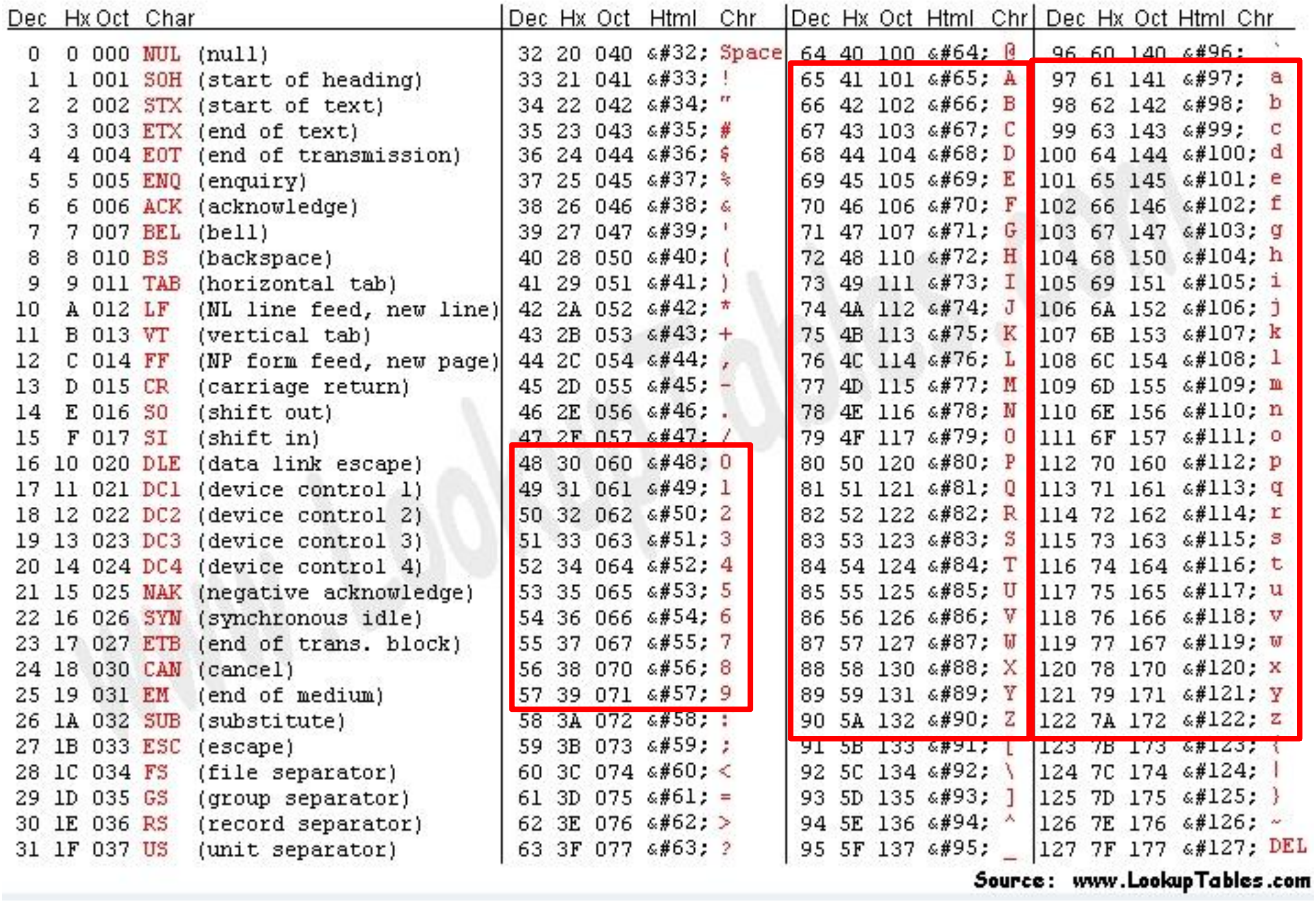
128	Ç	144	É	160	á	176	░	192	└	208	╨	224	α	240	≡
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	241	±
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
131	â	147	ô	163	ú	179	│	195	├	211	╙	227	π	243	≤
132	ä	148	ö	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
139	ï	155	¢	171	½	187	╗	203	╦	219	█	235	δ	251	√
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	

Source: www.LookupTables.com

The Mathematics of Strong Passwords

- **BUT WAIT**. . . Who uses all those “special” ASCII characters above 128, anyway? Who uses the Greek capital Sigma in a password? Or the square root sign? Which characters do we **REALLY USE**???

The Mathematics of Strong Passwords

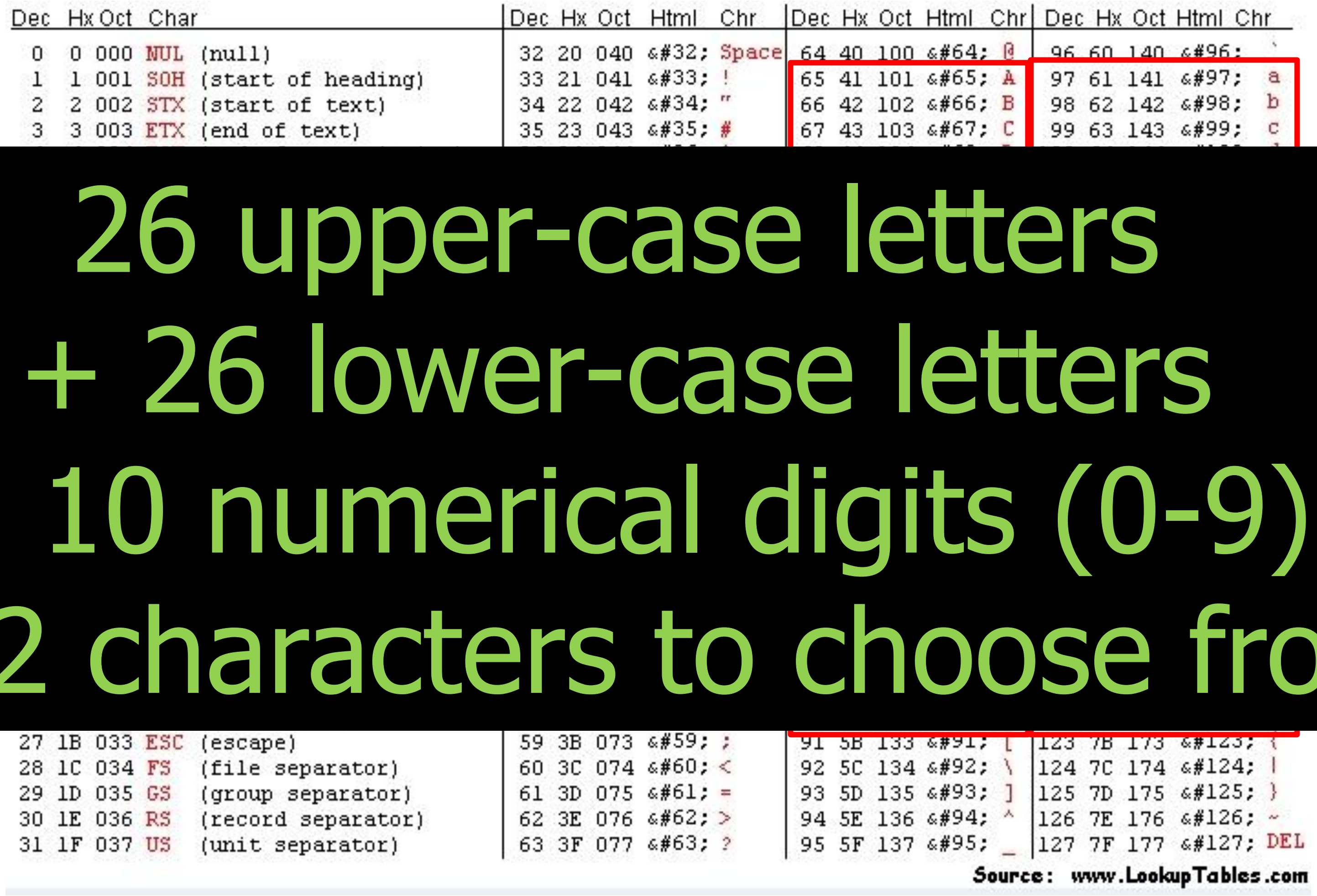


Dec	Hx	Oct	Char		Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL	(null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH	(start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX	(start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX	(end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT	(end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ	(enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK	(acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL	(bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS	(backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB	(horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT	(vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR	(carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO	(shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI	(shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE	(data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1	(device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2	(device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3	(device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4	(device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK	(negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN	(synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB	(end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN	(cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM	(end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB	(substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC	(escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS	(file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS	(group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS	(record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US	(unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Out of 256 available, we really only use 62 of them for passwords

The Mathematics of Strong Passwords



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c

26 upper-case letters
+ 26 lower-case letters
+ 10 numerical digits (0-9)
= 62 characters to choose from

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

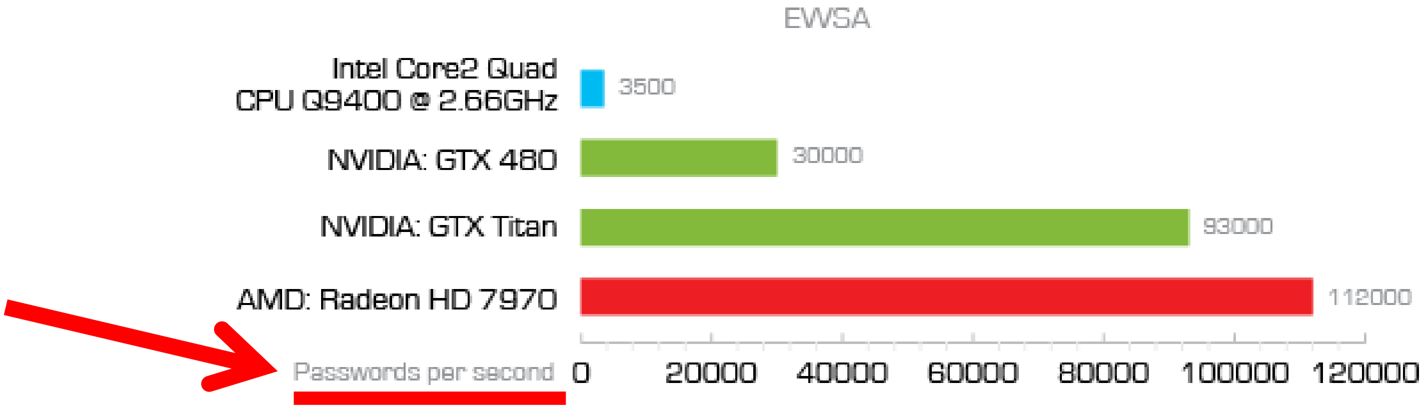
Out of 256 available, we really only use 62 of them for passwords

The Mathematics of Strong Passwords

- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)

The Mathematics of Strong Passwords

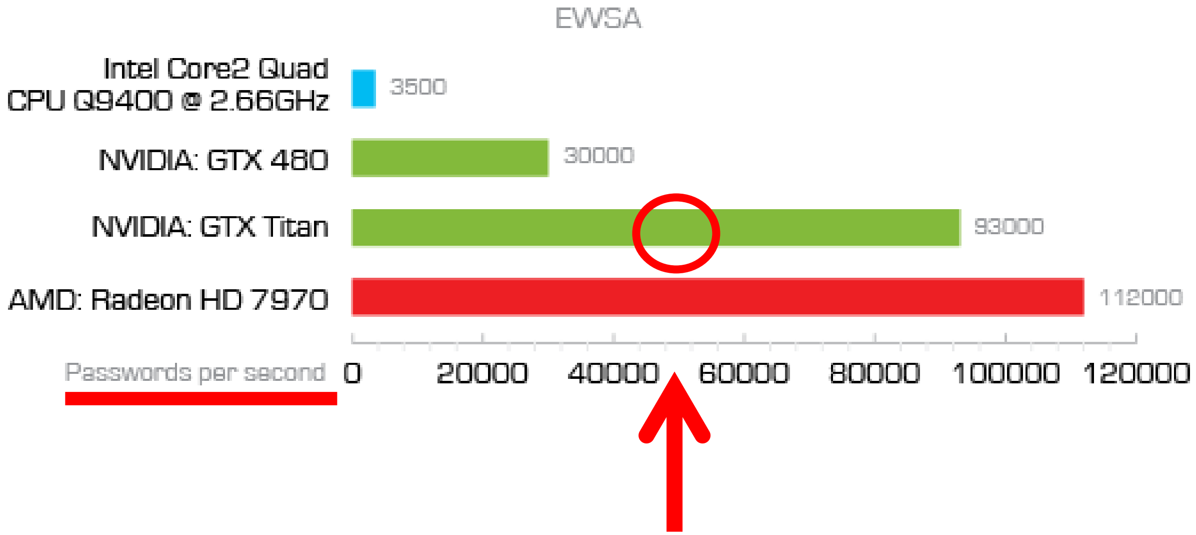
- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)
- How fast is a password cracking program?



(ref: http://www.elcomsoft.com/ewsa.html)

The Mathematics of Strong Passwords

- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)
- How fast is a password cracking program?
- We'll assume a "midgrade" cracker, capable of, say, ~50,000 passwords per second.



The Mathematics of Strong Passwords

- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)
- How fast is a password cracking program?
- We'll assume a "midgrade" cracker, capable of, say, 50,000 passwords per second.
- So, how long, ***on average***, will it take that midgrade cracker program to compromise a "typical" 5 ASCII character password?

The Mathematics of Strong Passwords

- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)
- How fast is a password cracking program?
- We'll assume a "midgrade" cracker, capable of, say, 50,000 passwords per second.
- So, how long, *on average*, will it take that midgrade cracker program to compromise a "typical" 5 ASCII character password?
- 916,132,832 total passwords/50,000 passwords-sec
- ≅ 18,322 seconds ≅ 5.1 hours (or 2.55 hrs average)

Assuming random choices for characters!

The Mathematics of Strong Passwords

- So instead of 256^5 = **1,099,511,627,776** possible passwords, we can really only generate:
- 62^5 = **916,132,832** possible passwords (0.083%!!)
- How fast is a password cracking program?
- We'll assume a "midgrade" cracker, capable of, say, 50,000 passwords per second.
- So, how long, *on average*, will it take that midgrade cracker program to compromise a "typical" 5 ASCII character password?
- 916,132,832 total passwords/50,000 passwords-sec
- ≅ 18,322 seconds ≅ 5.1 hours (or 2.55 hrs average)

*THIS IS CALLED A **"COMBINATORIAL ATTACK"***

The Mathematics of Strong Passwords

- But why bother with obscure, randomized words? They are ***so*** hard to remember! ***Who has the time***?

The Mathematics of Strong Passwords

- But why bother with obscure, randomized words? They are so hard to remember! Who has the time?
- Just choose a word from the dictionary, right? Easy to remember and saves me time (“**I got places to go, people to see, things to do**!”)

The Mathematics of Strong Passwords

- But why bother with obscure, randomized words? They are so hard to remember! Who has the time?
- Just choose a word from the dictionary, right? Easy to remember and saves me time ("I got places to go, people to see, things to do!")
- There are about 470,000 words available in the English language (ref: http://www.merriam-webster.com/help/faq/total_words.htm)

The Mathematics of Strong Passwords

- But why bother with obscure, randomized words? They are so hard to remember! Who has the time?
- Just choose a word from the dictionary, right? Easy to remember and saves me time ("I got places to go, people to see, things to do!")
- There are about 470,000 words available in the English language (ref: http://www.merriam-webster.com/help/faq/total_words.htm)
- Assuming that all of these words might also start with a capital letter, that gives us an additional 470,000 possibilities, for **940,000** total candidate passwords.

The Mathematics of Strong Passwords

- **NOW** Let’s see how the cracking program fares. . .

The Mathematics of Strong Passwords

- **NOW** Let’s see how the cracking program fares. . .
- Assume the author of the password cracker is smart.

The Mathematics of Strong Passwords

- **NOW** Let's see how the cracking program fares. . .
- Assume the author of the password cracker is smart.
- He (or she) tries dictionary words **first**, before launching into a combinatorial attack. Trying dictionary words is called a "***dictionary attack***".

The Mathematics of Strong Passwords

- **NOW** Let’s see how the cracking program fares. . .
- Assume the author of the password cracker is smart.
- He (or she) tries dictionary words first, before launching into a combinatorial attack. Trying dictionary words is called a “dictionary attack”.
- Now how long to crack your password?

The Mathematics of Strong Passwords

- **NOW** Let's see how the cracking program fares. . .
- Assume the author of the password cracker is smart.
- He (or she) tries dictionary words first, before launching into a combinatorial attack. Trying dictionary words is called a "dictionary attack".
- Now how long to crack your password?
- 940,000 PWs/50,000 PWs-sec (÷2 for average time)
- ≅ 9.4 seconds … wow! Less than 10 secs!
- **Compare: 2.55 hours vs. 9.4 seconds.**

The Mathematics of Strong Passwords

- **NOW** Let's see how the cracking program fares. . .
- Assume the author of the password cracker is smart.
- He (or she) tries dictionary words first, before launching into a combinatorial attack. Trying dictionary words is called a "dictionary attack".
- Now how long to crack your password?
- 940,000 PWs/50,000 PWs-sec (÷2 for average time)
- ≅ 9.4 seconds
- **Compare: 2.55 hours vs. 9.4 seconds.**
- **Security is reduced by a factor of about 1000!**
- **… 1,000 TIMES LESS SECURE**

when choosing dictionary words compared with random choices for characters!

The Mathematics of Strong Passwords

- **Compare: 2.55 hours vs. 9.4 seconds.**
- **Security is reduced by a factor of about 1000!**
- **… 1,000 TIMES LESS SECURE**

when choosing dictionary words compared with random choices for characters!

- If some ***special characters*** are included (e.g.: % , $, & , #, ! , @ , { , } , < , > , ?), then that 2.55 hours **increases**.
- Increasing the time required for an attacker to compromise your password gives GMU's IT Security a fighting chance to detect and block that illegal action.
- 2.55 hours vs. 9.4 seconds!

Okay, what were we talking about?...

I.T. Ethics (the "2+2 perspective")

1. **The good guys**
   - Things that we do (but SHOULDN'T)
   - Things that we don't do (but SHOULD)

2. **The bad guys**
   - Things that they do in a passive mode
   - Things that they do in an active mode

Reference: http://www.auburn.edu/~fordfn1/aces5770.html

Remember: PII = Personally Identifiable Information

Other Things That Bad Guys Do . . .

Reference: http://www.imvajra.com/glossary1.html

- Passive:
  - Cookies (… however, non-identifying tracking is okay)
  - Web Beacons (single pixels on webpage or in an email)
- Active:
  - Hacking (e.g., unauthorized access to computer or network)
  - Spam (unsolicited email; e.g., scam you out of your money)
  - *Phishing* (for passwords, account numbers, PII)
  - Even more insidious: "***Spear Phishing***"
  - Fraud (obtaining goods, services, or property through ***deception or trickery – "Social Engineering"***)
  - Worms, Viruses, and Trojans (= death to your computer, and maybe death to the whole network!). Also corrupts data!
  - DoS attacks (= Denial of Service)
  - Spyware, including click-loggers (i.e., keystroke logging)

“Spear Phishing” Defined

- What the heck is “***Spear Phishing***?” (sounds like fun, actually!)
- From the FBI’s website:

“Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The e-mails appear to be sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive.”

(ref: http://www.fbi.gov/news/stories/2009/april/spearphishing_040109)

Real-Life "Spear Phishing" Examples at Mason (I)

- **Appeared in "ITU SUPPORT CENTER ALERTS" on 6 Oct 2011:**

SUBJECT: Re: Upgrade Your Eamil

George Mason University

Attention GMU Webmail User,

This is to bring to your notice that because of the incesant rate of spam mails we are upgrading our database and you will be required to click on the below url to make your account upto date:

[LINK REMOVED FOR YOUR SAFETY]

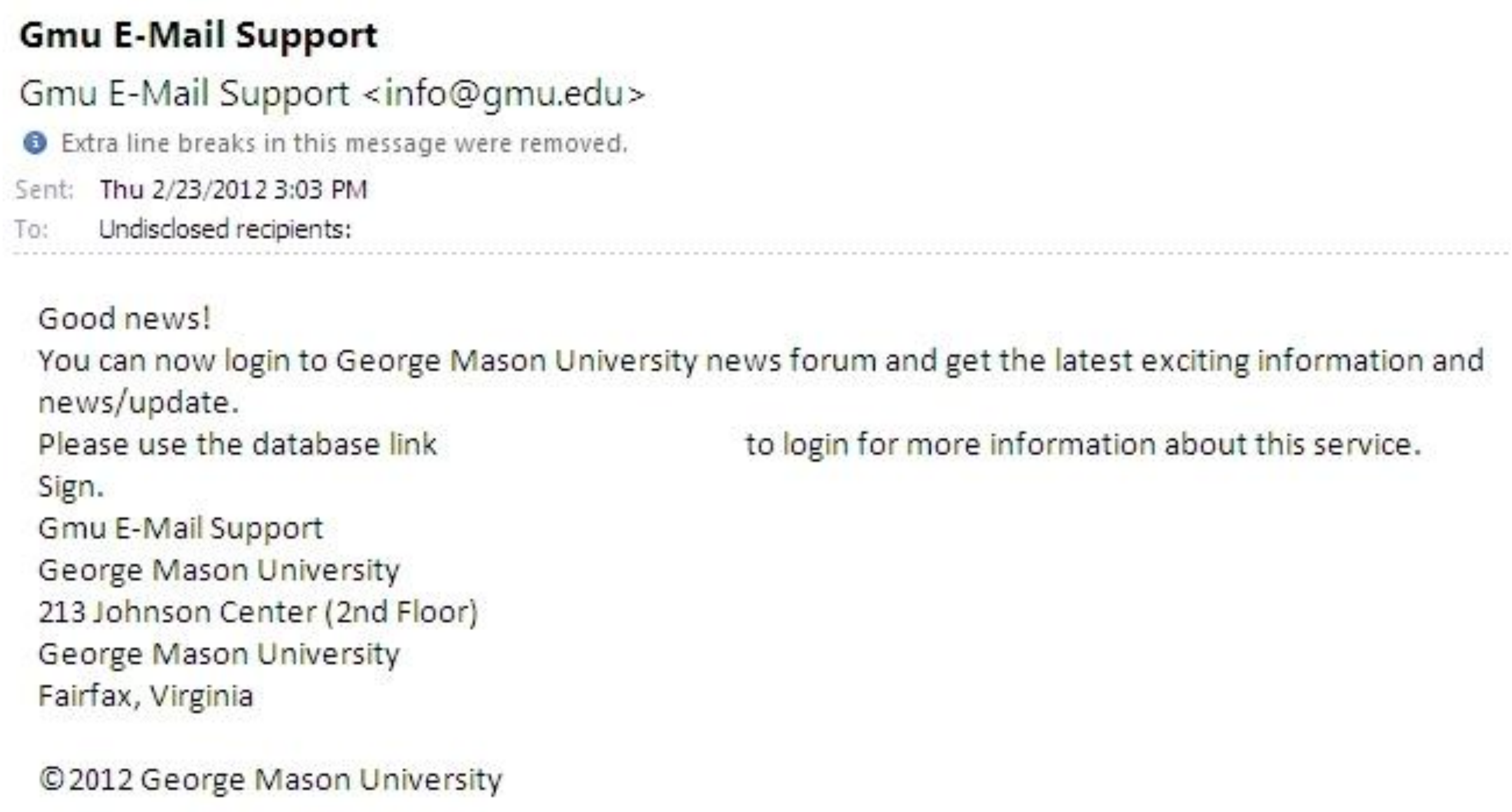
Thanks for pakaking and we hope to serve you better.

Warm Regards,

GMU HelpDesk.

Real-Life “Spear Phishing” Examples at Mason (II)

- **Appeared in selected GMU email inboxes on 23 Feb 2012:**



Gmu E-Mail Support

Gmu E-Mail Support <info@gmu.edu>

Extra line breaks in this message were removed.

Sent: Thu 2/23/2012 3:03 PM
To: Undisclosed recipients:

Good news!
You can now login to George Mason University news forum and get the latest exciting information and news/update.
Please use the database link to login for more information about this service.
Sign.
Gmu E-Mail Support
George Mason University
213 Johnson Center (2nd Floor)
George Mason University
Fairfax, Virginia

©2012 George Mason University

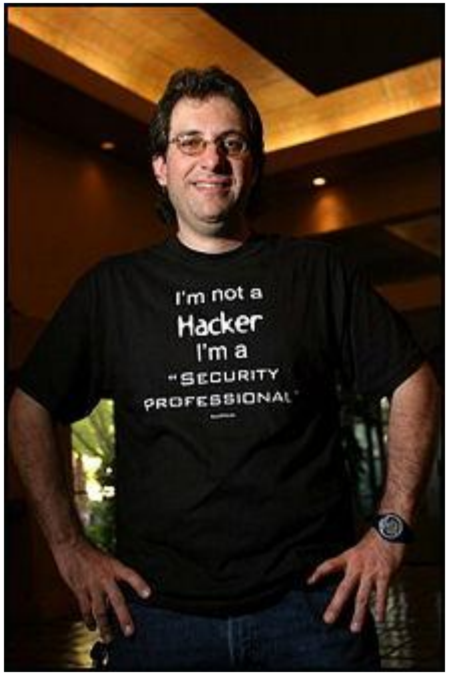
“Social Engineering” Defined

- What the heck is ***Social Engineering?*** (sounds like fun!)
- It isn’t fun…
- …and it isn’t a Degree Program in Mason’s Engineering School.
- From Wikipedia:

“**Social engineering**, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information”

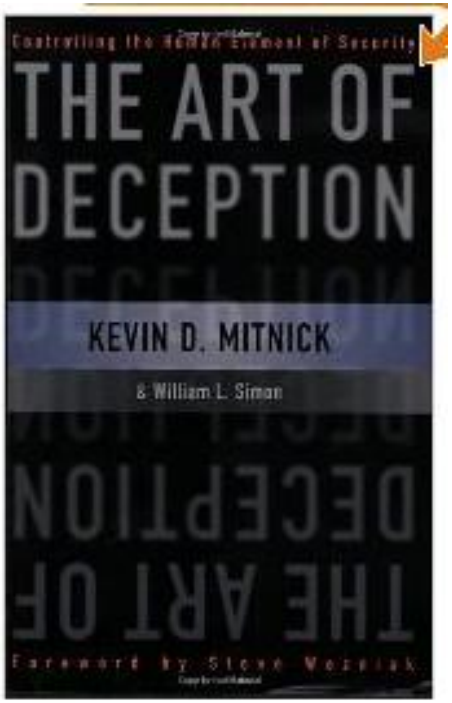
(ref: http://en.wikipedia.org/wiki/Social_engineering_(security))

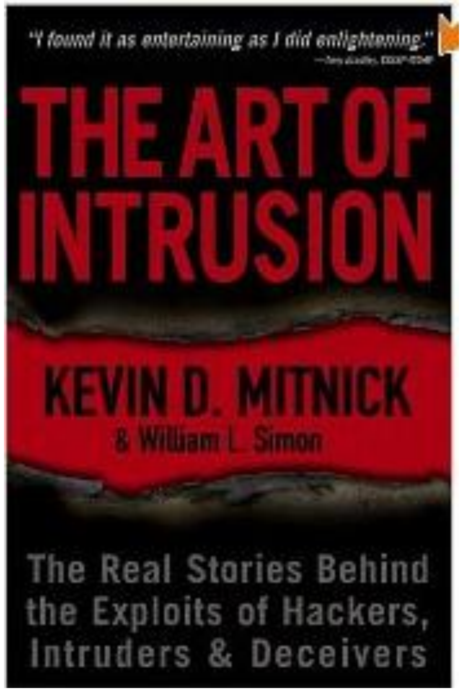
Great Books . . . Unfortunately!



Kevin Mitnick

The original
social engineer


Controlling the Human Element of Security
THE ART OF
DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak



(refs: http://en.wikipedia.org/wiki/Kevin_Mitnick and Amazon.com)

Also Beware of Malicious Insiders . . .

- **"The Insider Threat" is the top security concern for companies**
- Estimated **85%** of all fraud is committed by employees
  - This may be due to collusion (cooperation) between an employee and an outsider
  - Increasingly common among fired (or otherwise disgruntled) employees
    - … especially an I.T. tech!
  - Watch the 1999 movie "Office Space" (for a dark comedic twist)
- Usually due to weaknesses in internal controls.
- Very difficult to detect and to stop
  - These people are authorized to access the very systems they abuse!
- Insiders are not always employees . . .
  - Can also be consultants, contractors, or *anyone with access*.

Final Remarks – Your Responsibilities…

- The general public does not realize the critical importance of IT ethics.
- Important ethical decisions are often left to technical experts.
- Each one of us must assume greater responsibility for these decisions.
- Our decisions must be informed and objective, based on technical knowledge, an understanding of the challenges, and a sense of ethics.
- Each of us must also try to create and sustain an environment of trust, in which ethical dilemmas can be discussed openly, objectively, and resolved constructively.