

They Know What?!?: Security & Privacy in the Internet Age

R. Scott Granneman

scott@granneman.com

www.granneman.com

© 2004 Scott Granneman

Last updated 20040912

You are free to use this work, with certain restrictions.
For full licensing information, please see the last slide/page.

Security is a process,
not an event.

You might think that security is hard.

Lots of things are harder.

(To be considered a master ventriloquist,

you must be able to “say” this:

“Who dared to put wet fruit bat poo

in our dead mummy's bed;

was that you, Verity?”

– now *that's* hard!)

You might think that computers are confusing
& make your head spin.

You might think
you've got
too much
on your mind
to think about
security.

You might think you're doomed
no matter what you do.

You might think security doesn't relate to you.

Here's a story that happened less than a week ago:

Judith's friend is stalked by her ex.

You might think that your computer,
or your information,
is an insignificant part of the whole.

Ever try to open a bag of chips
that just won't open?

You pull & twist & tear,
& it won't open.

Then you make a tiny rip with your teeth,
& the bag opens easily,
so that all the chips are yours.

Your computer is the tiny rip
in your school's network.

There are several things you can do
to protect yourself.

Most are pretty easy.

Pick a good password.

“John the Ripper”

(<http://www.openwall.com/john/>)

will make mincemeat of poor passwords.

The guidelines:

1. Don't use easy passwords
2. Mix of 3 of these 4: A a 1 #
3. At least 8 characters
4. Easy to remember & hard to guess

Here's a good method for picking a good password:

“There's a lady who's sure all that glitters is gold”

Talwsatgig



Ta1w5atg1g



Ta1w5atg1g!

“I'm gonna fight 'em off,
A seven nation army couldn't hold me back”



1gfeθ, A7nachm6

“Somewhere over the rainbow, way up high”



Sθtr, wuh

“Shut up Just shut up Shut up”



SuJsuSu

If you use Windows,
set up Windows Update to automatically update
your computer.

Search Google for
“set up automatic windows update”

If you use Microsoft Office,
check the Office Update web site periodically.

<http://office.microsoft.com/en-us/officeupdate/>

If you use Windows,
you must run the following:

Anti-virus software

Anti-spyware software

A personal firewall

(If you use Mac OS X or Linux,
you really don't need to worry about viruses or spyware.)

It's not enough to have anti-virus software.

You must set it to automatically
update the virus database every night.

You must set it to automatically
scan your computer every night.

Don't get fooled by virus hoaxes.

There is no virus with a teddy bear logo
& the name jdbgmgr.exe.

There is no Good Times virus.

But *do* beware of the Bad Times virus!

If you receive an email with the subject line "Badtimes" delete it IMMEDIATELY. This is the most dangerous email virus yet.

Not only will it completely rewrite your hard drive, but it will scramble any disks that are even close to your computer. It reprograms your ATM access code and uses subspace field harmonics to scratch any CDs you try to play. It will recalibrate your refrigerator's coolness settings so all your ice cream melts and your milk curdles. It will give your ex-boy/girlfriend your new phone number. It will drink all your beer. You will have nightmares about circus clowns. It will replace your shampoo with Nair, leave the toilet seat up, and leave your hairdryer plugged in dangerously close to a full bathtub.

You have been warned!

If you receive a warning about a virus,
check it out first:

<http://www.vmyths.com/hoax.cfm>

<http://www.snopes.com>

<http://www.granneman.com/techinfo/email/hoaxes/>

Don't engage in the kind of risky behavior
that will get you infected with a virus.

Don't open attachments you weren't expecting.

Don't install shady software.

As a side note,
configure Windows to show all file extensions.

That way you'll know the difference between

anna-k.jpg

&

anna-k.jpg.bat

Instructions:

<http://www.granneman.com/techinfo/>

[windows/showextensions/](http://www.granneman.com/techinfo/windows/showextensions/)

People that make spyware
should be hung by their thumbs.

Spyware: “software that gathers information
about a computer user
and then transmits this information
to an external entity
without the knowledge or informed consent
of the user.”

<http://en.wikipedia.org/wiki/Spyware>

How do you get spyware?

1. You install software that includes spyware.
2. Drive-by installs via your Web browser.

From the KaAaA End User License Agreement:

“9.1 During the process of installing Kazaa, you must install software from third party software vendors pursuant to licences [sic] or other arrangements ... Please note that the Third Party Software may be subject to different licences or other arrangements, which you should read carefully. By installing and using this Third Party Software you accept these Third Party Software licences or other arrangements and acknowledge that you have read them and understand them. Sharman does not sell, resell, or license any of this Third Party Software, and Sharman disclaims to the maximum extent permitted by applicable law, any responsibility for or liability related to the Third Party Software. Any questions, complaints or claims related to the Third Party Software should be directed to the appropriate vendor.”

“9.4 Embedded Third Party Software

9.4.1 ... Cydoor Technologies advertising delivery program, which may display web content such as banner ads, e-commerce offers, news headlines and other value-added content. ...

9.4.4 ... The GAIN AdServer software identifies your interests based on some of your computer usage and uses that information to deliver advertising messages to you. ...

9.4.5 ... PerfectNav is designed to redirect your URL typing errors to PerfectNav’s web page.”

How can you avoid spyware?

Watch what you install on your computer.

Search Google to see if anyone reports spyware with the program you're thinking of installing.

Always do a Custom Install,
which will show you
what programs are getting installed.

Don't use Internet Explorer.



In fact, avoiding Internet Explorer
is just good all-around advice.

Internet Explorer is chronically
buggy & insecure.

Microsoft hasn't improved IE for almost 4 years.

And forget about any downloadable upgrades
in the future.

There are several browsers
that are safer & more secure,
& have far better features
than Internet Explorer.

Mozilla & Firefox



(Windows, Mac OS X, Linux)

<http://www.mozilla.org>

Opera

(Windows, Mac OS X, Linux)

<http://www.opera.com>

Safari

(Mac OS X)

<http://www.apple.com>

You may still need to use Internet Explorer
on a few web sites.

Online banking, for instance.

Use IE *only* for those sites & no others.

Test the security of Internet Explorer
if you're going to continue to use it.

<http://www.pcflank.com/about.htm>

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

Good anti-spyware software is free & easy to use.

Ad-aware

<http://www.lavasoftusa.com/software/adaware/>

Spybot Search & Destroy

<http://spybot.safer-networking.de/en/>

Don't forget
to run your anti-spyware software often.

Don't forget to update your anti-spyware software
every time you run it –
new spyware comes out all the time.

(You can purchase anti-spyware software
that will automate these tasks.)

Run personal firewall software.

Windows XP comes with a built-in firewall,
but it's not turned on by default.
Service Pack 2 fixes this defect.

However, it only blocks inbound connections,
so outbound connections are still a problem.

Mac OS X & Linux include good firewalls.
Windows users should look at one of these:

Kerio Personal Firewall

http://www.kerio.com/kpf_download.html

Sygate Personal Firewall

http://smb.sygate.com/products/spf_standard.htm

ZoneAlarm

[http://www.zonelabs.com/store/content/company/
products/zna1m/freeDownload.jsp](http://www.zonelabs.com/store/content/company/products/zna1m/freeDownload.jsp)

In addition to firewall software on your computer,
you really should purchase
a hardware router/firewall.

They're cheap now –
many are less than \$50 –
they're easy to set up,
& they really work well.

Linksys, D-Link, Netgear, Belkin:
they're all good.

Don't forget to change
the default administrator password
on your firewall!

Default passwords are well known.

Maker	Device	Login	Password
Apple	Airport 1.1	-	public
D-Link	DI-704	-	admin
Intel	Wireless 2011	-	Intel
Linksys	Cable/DSL router	-	admin
Netgear	RT311/RT314	admin	1234
SonicWall	Any firewall	admin	password

<http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php>

After you install your firewall,
test it using any of these web sites:

<http://www.dslreports.com/scan/>

<https://grc.com/x/ne.dll?bh0bkyd2>

<http://hackerwhacker.com:4000/startdemo.dyn>

If you use the Internet,
it's pretty easy to spy on you



... unless you take some precautions.

Don't fall for *social engineering*.

Social engineering,

AKA,

people will tell you anything
if you sound authoritative.

Ants recognize friends & foes by smell.

Beetles sneak into ant colonies,
play dead if they're attacked,
& get the ants' smell on them.

Once they smell like an ant,
they can wander about the colony,
eating ant larvae.

What's the easiest way to get
sensitive information from people?

Just ask.

“This is campus IT support. We’ve had a problem, & we need to reset everyone’s passwords on the network. What’s your current username? Good. And your current password? OK, thanks. Your new password will be 123456. Try that in 24 hours after we’ve fixed the problem.”

True story:
a woman posts an ad looking for a nanny.
References & full resumé required.

Nanny responds, sending all info.
Woman never responds to nanny.
“Oh well,” nanny thinks.

Woman turns around &
posts an ad looking for a job as a nanny.

Guess whose references & resumé she uses?

Then there's *phishing*.

Example from http://www.antiphishing.org/phishing_archive/ebay1.htm

From: SecretService@ebay.com

Sent: Sat 10/25/2003 1:50 PM

To:

Cc:

Subject: eBay Member Billing Information updates



My eBay

[? Need Help?](#)

Dear eBay Member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our website [eBay Billing Center](#) and fill out the proper information that we are needing to keep you as an eBay member.

If you think you have received this email as an error, please visit our website and fill out the necessary information. That way we can make sure that everything is up to date! Again here is the link to our website. [eBay Billing Center](#)

Please Do Not Reply To This E-Mail As You Will Not Receive AResponse

Thank you
Accounts Management

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our [Privacy Policy](#) and [User Agreement](#) if you have any questions.

[Announcements](#) | [Register](#) | [Safe Trading Tips](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright ?1995-2003 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the [eBay User Agreement](#) and [Privacy Policy](#).



Security Update

[? Need Help?](#)



For security reasons the following information must be confirmed.

eBay User ID

You can also use your registered email.

Password

Please re-enter your email Address:

Please re-enter your Social Security Number (SSN)

(The SSN consists of nine digits, commonly written as three fields separated by hyphens: AAA-GG-SSSS)

Important: In order to prevent any fraudulent activity from occurring we strongly advise you to specify an alternative eBay password. This process allows us to give back sole control of the account to you in case something goes wrong with instructions regarding the account and its future safety.

Alternative password (6 character minimum)

Please note that when choosing a password we strongly recommend that you choose a password that can be easily remembered.

⚠ Please confirm your credit or debit card on file to help verify your identity. Your information is kept safe and private. 🔒

Please make sure your card expiration date is correct.
If your card has expired, please enter another one.

Full Name on Credit Card:

Credit Card Billing Address:

City:

State/Province:

Province if not US/Canada:

Zip/Postal Code:

Phone Number:

Fax Number:

Country:

Important: If necessary, please edit the above information to match your credit card billing information.

Card Type:

Visa, Mastercard, American Express, or Discover
Your card will not be charged!

Card Number:

Expiry (mm/yyyy):

CVV2 code

The CVV2 code is the three-digit code on the back of the card following your credit card number.

ATM PIN (Bank Verification) #:

Submit

Companies like Amazon, eBay, PayPal,
Yahoo, & Microsoft
will never send you emails asking you
to verify sensitive information.

When in doubt, pick up the phone
& call them.

Ask.

Another easy way to get sensitive information:

Look for it.

No one here posts sticky notes
with their password on them,
right?

Naaah.

You hide 'em under your keyboard,
where no one would *ever* think to look.

Garbage cans are a gold mine of useful information.

Bank statements

Credit card statements

Paycheck stubs

Personal letters

Applications

Transcripts

Org charts

Contact lists

Memos

Reports

Floppies

CDs

Hard drives

One scenario:

Your network admin gets an anonymous call:
people are posting passwords on sticky notes.

The word goes out to all employees:
take down your sticky notes!

And the office dumpster is now brimming
with password-filled scraps of paper.

If you want to throw something out
that contains sensitive info,
shred it.

You can buy reconditioned shredders
on eBay for \$35.

Use a wireless network?

Free, open wireless networks
are popping up everywhere.

Oh, it's sooooo easy to grab information from folks
using open wireless networks.

Let me tell you a story:
Matt & the cute girl at the coffee shop.

What's a sniffer?

A program and/or device
that monitors the data passing through a network.

It can tell the user
where data is coming from,
where data is going,
and what the data is.

If the program you're using to access the Internet
isn't using encryption,
then you're vulnerable to a sniffer.

Email.

Web.

IM.

All unencrypted (most of the time).

All vulnerable.

If you're using a wireless network,
assume that someone is standing over your shoulder
watching every single thing you type.

(Or, if you're a nerd,
tunnel your traffic through SSH.)

Be careful when using Internet cafés
& computer labs.

Bad guys install *keyloggers* on those computers.

Hardware keyloggers are easy to spot –
if you know where to look.

Software keyloggers are much harder to detect.

A major annoyance we all live with:

We're all getting way too much spam.

Subject	Sender	Date	Size
JUNK OnlinePharmacyCheap	Lucio Bennett	2004-09-12 1:13 am	2.4 KB
JUNK Premium Cigars, Travel Case, and Cutter - All for \$29.95	Thompson Cigar	Today 9:25:32 am	10.4 KB
JUNK Record better with a Sony Handycam □ optical & digital zoo...	Cool Camcorders	Today 9:03:06 am	8.2 KB
JUNK V1AGKRA 80% DISCOUNT !!	Rodger Farris	Today 8:54:00 am	2.7 KB
JUNK Want to lose up to 19% weight. Try Adipren!	Tracy McGraw	Today 10:21:46 am	2.6 KB
[cwe-lug] [Fwd: [Dee-Ann general] Free online classes starting again]	Jerry Hubbard	Today 7:59:30 am	3.9 KB
[Editors] Make money for your opinions!	Online Surveys	Today 9:36:19 am	4.7 KB
[Editors] Ref:--REO Realty Income--- B	Carmencita	Today 9:31:14 am	2.8 KB
[Editors] Survey Finds Prescription Drug Abuse Up 15 Percent Among Y...	Narconon Arrowhead	Today 10:11:21 am	13.3 KB
[Editors] This could change everything	Online Careers	Today 7:59:09 am	4.8 KB
[Editors] Постер-трансформер - это новое оружие мерчендайзера с...	alejandr	Today 8:32:01 am	6.5 KB
RE: [TheDude] Mantis!	Tyler S. Harris	Today 9:32:49 am	12.3 KB
Re: [wwwac] Hopefully simple Javascript question	Tom Simpson	Today 7:54:09 am	2.8 KB
Re: [wwwac] Web Site Analysis Software (Humor-Endowed)	Frank D. Greco	Today 8:39:52 am	2.1 KB
Re: [wwwac] Yahoo goes consumer electronics?!?!	David W. Fenton	Today 10:25:30 am	2.8 KB
AMATEUR INCEST VIDEO SITE	Wendi@morelos.com	Today 10:50:10 am	1.2 KB
Bill Received from LACLEDE GAS COMPANY	Support@paytrust.com	unknown	2.1 KB
Bryan Consulting server down	rsgranne@bhoth.pair.com	Today 8:40:12 am	781 B
Busy Night	Jans Carton	Today 8:06:39 am	1.4 KB
Cable Box Unlocked	Earnest Hinkle	Today 8:40:07 am	1.9 KB
Delivery reports about your e-mail	john@cavaliers.org	Today 8:22:01 am	40.3 KB
Does Pain Affect Your Job Performance? NTEX	annalisa smock	Today 9:33:18 am	2.4 KB
Fill 'er up for less	SaveAt ThePump-JustFor ...	Today 7:54:35 am	4.8 KB
Get a \$175 Silver Bracelet from a World Famous Jeweler - for nothing	Fifth Avenue Jewelers	Today 8:34:34 am	4.8 KB
luck,St0cks in Play	Walter Flynn	Today 9:51:00 am	8.1 KB
Microsoft disc ounts	galexand@pkl.net	Today 10:15:33 am	1.3 KB
New Message: Spring 2004: Advanced Web Site Design and Developme...	scott@granneman.com	Today 8:29:05 am	23.7 KB
Re: Problem installing Windows 2000 in Bochs	David Pye	Today 10:00:38 am	3.0 KB
Ralph, Meet serious CHRISTIAN SINGLES, just like you	Where CHRISTIANS Meet	Today 9:55:26 am	11.7 KB
ralph; Need a laptop? Get a free IBM Thinkpad!	lagnernow	Today 11:33:00 am	3.5 KB
Roxio Easy Media Creator 7	roxio7	Today 8:41:13 am	3.3 KB
Re: Site Structure display failure	Jans Carton	Today 8:03:04 am	2.6 KB
Watch Your Wall Paper Come Alive	Screen Saver Deals	Today 9:59:47 am	3.9 KB
Where Do the Professionals Go For Results?	Marketing Guru's BVM	Today 9:42:24 am	3.4 KB

How do spammers get your email address?

Posts on web sites

Submissions to web sites

Posts on Usenet (newsgroups)

Collections of email addresses bought & sold
among spammers

“Why Am I Getting All This Spam?” Center for Democracy & Technology. March 2003.

<http://www.cdt.org/speech/spam/030319spamreport.shtml>

How can you ~~stop~~ reduce spam?

Never respond to spam,
especially to “unsubscribe”.

My buddy David Hale’s dad
found this out the hard way.

Don't post your email address on the Web!

If you must, encode it.

scott at granneman dot com

HTML Character Entities

pcoqq@goanneman.com

@ = @ . = .

a = a b = b c = c

etc.

Encode your email address:

<http://www.wbwip.com/wbw/emailencoder.html>

```
<script type="text/javascript">
// generate your own at http://hiveware.com/enkoder_form.php?real
//<![CDATA[
function hiveware_enkoder(){var i,j,x,y,x=
"x=\"1Ex8A=\\\"7}1e83;x7q;=8j9\\\"7s\\\"88l};5yB88m'6<@<88n=;908;8Bi:;7788.\" +
\"77>%8882;5<2888~9;90888B;9;z;8;s;;8j8;8x;;h888f8<:u888j<98-88;, :79*888,;5\" +
\":0;8;}9;83888x;87z888g::7x8;8y;;9w;88-:::n8;81<9;788;.989.8;8@78;$;88~:76\\\" +
\"\\\"8;\\\"8<;;88y8<=>88'8<6';88;;78x88;=8;:u788n8>7e588s8<7c:88a897p888e8;\" +
\">(;88x8:8)88;;877f;88o;=8r;88(875i<88=878098;;887i<;7<887x988.8;gl:8<e;6>n\" +
\"888g87it787h85<;787i8;<+888+;=g):8;{8<;j<8;=87kx88<.8;7c;87h8:=a88;r8;>C;8\" +
\"8o;;id;88e885A<;8t89g(98;i8:>)<;8-88h598<;87=i787f87j(58;j8;h<;;389:268;)\" +
\"8;jj<8;+86<=98<98;9478;;8>=y588+8;g=;;;588>t<87r8<gi<88n89ig788.8;7f;;7r8;\" +
\">o68<m88gC;;<h;6>a:87r8<gC;88o;8id:8<e8;:(;8;j88j):8;}8;:y\\\"; <;j;8=e8;va\" +
\"<8l(8;x.96ch8<ar<5At8;(09:))87;x9==x87.s5<ub87st;:r(871)<<;y87='<g';8<fo7=\" +
\"r(87i=;j0;8<i<68x.8<le::ng;;th:7;i8<+=;82);<{y:9+=8<x.;7su87bs:=tr8;(i;>,1\" +
\";7);9h}f88or;7(i87=16>;i87<x;>.l;8en:ggt8<h;7ii+;<=2:>){8'y+;@=x8~.s8Bub8,\" +
\"st;,r(;@i,;k1)8t;};wy=-y.9nsu8Bbs:5tr;@(j8n);\\\";j=eval(x.charAt(0));x=x.s\" +
\"ubstr(1);y='';for(i=0;i<x.length;i+=4){y+=x.substr(i,2);}for(i=2;i<x.lengt\" +
\"h;i+=4){y+=x.substr(i,2);}y=y.substr(j);\";
while(x=eval(x));}hiveware_enkoder();
//]]>
</script>
```

Encode your email address:

http://hiveware.com/enkoder_form.php

If you submit your email address
using an online form:

1. Opt out of email
(& give 'em as little real data as necessary)

2. Tag your email

If a form wants personal data,
only give 'em what is absolutely necessary.

Don't feel like you have to be honest
about your whole life.

Remember:
data about you
isn't owned by you –
it's owned by whoever collected it.

If you submit your email address
using an online form,
opt out of email.

If a company violates its privacy policy,
report it to the Federal Trade Commission.

<http://www.ftc.gov>

Tag your email
so you know if a web site sells your address.

scott+amazon@granneman.com
scott+ebay@granneman.com

Use a disposable email address.

Yahoo, Hotmail, & others
offer free email services.

Search Google for “disposable email address”
for services that offer 100s of email addresses
you can use & toss.

Set up email filters.

If you're a nerd, use SpamAssassin & procmail.

Don't know what SA & procmail are?

Then you're not a nerd.

(If you want copies of my procmail files, just ask.)

If you're a non-nerd,
use an email program that supports
Bayesian filters.

Bayesian filters are “trained” over time
to recognize what you consider spam
& what you do not.

Email programs with built-in Bayesian filters:

Thunderbird (Windows, Mac OS X, Linux)

<http://www.mozilla.org/products/thunderbird>

Mozilla Mail (Windows, Mac OS X, Linux)

<http://www.mozilla.org>

mail.app (Mac OS X)

<http://www.apple.com/macosx/features/mail/>

(By the way,
these email programs all tend to be far more secure
than Outlook or Outlook Express.)

Add Bayesian filters to your email program:

SpamBayes, for Outlook
(Windows)

<http://spambayes.sourceforge.net>

POPFile, for Eudora, Outlook, Outlook Express,
& others

(Windows, Mac OS X, Linux)

<http://popfile.sourceforge.net>

The big problem with security:
most people don't work well with formal methods.

If it's too difficult, or too "rigid",
people won't do it –
or they relax it to allow for "circumstances".

Ever bought something online?
Did you check to make sure the web address
used “https” instead of “http”?
Or look for the little gold lock?

Most people do.

It's easy. No work is involved.

Now, how many of you encrypt your email?

Thought so.

Security is a process,
not an event.

To be effective,
security has to be a way of life.

Thank you!

Email me: scott@granneman.com

Visit my Web site: www.granneman.com

Publications: www.granneman.com/pubs

My blog: www.granneman.com/blog



Licensing of this work

This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/1.0> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

In addition to the rights and restrictions common to all Creative Commons licenses, the Attribution-ShareAlike License features the following key conditions:

Attribution. The licensor permits others to copy, distribute, display, and perform the work. In return, licensees must give the original author credit.

Share Alike. The licensor permits others to distribute derivative works under a license identical to the one that governs the licensor's work.

Questions? Email scott@granneman.com