

From Fred Showker's Nationally published column...

Password is NOT a 4-letter word

Yesterday, a close relative's identity was stolen.

The whole ordeal and the ensuing headaches of identity theft has prompted me to write and once again to remind everyone about online safety. Folks, it's not a matter of "if" they will discover your password -- but "when". Below, I emphasize the iron-clad rules of dealing with passwords.

This person used a cat's name as a password in an eBay account less than a year old. And that's all it took for a criminal to crack into ebay, begin posting bogus items for sale and using the credit card account. We may not have even discovered it had it not been for an unwary user who emailed with questions about one of the bogus offers. The relative called me and said "I've got this email from eBay about a product I'm not even selling." I knew at once what happened. We jumped on it and were able to stop it before the real disaster could happen.

Never underestimate the online criminal.

These criminals employ sophisticated software and servers to rapidly harvest screen names from eBay, Amazon, blogs, and anywhere a "handle" or screen name is used. Incoming data is then compared to databases with millions of words, phrases, acronyms, street addresses and telephone numbers. It takes only a few seconds to then ping eBay and other online strongholds to test combinations. Once a 'hit' is made, they're in. It's only a matter of time.

These are not isolated hackers crouched at a glowing monitor in the dead of night -- they're technologists and industrialists exploiting all means available. They're highly skilled and well financed businesses openly bragging that they can't be caught, and can't be stopped. They employ major computer installations

which run around the clock, every day -- fully staffed for a single purpose: stealing and exploiting private information.

Online crime has been cited as one of the worlds most rapidly expanding industries -- transcending borders and language. The spam, porno and identity theft business has become so lucrative it can employ the fastest and most advanced technologies. Their multi-computer installations can parse millions of screen names and email accounts per hour, matching them to spam lists as well as gathered cookies from anyone who surfs the web. They employ intelligent agents and spiders to scour the web for possible UID and cookie matches. When a match is found, they sell it; use it to create more bogus accounts for spamming; or even worse, use it to burglarize bank accounts and charge card accounts. In this particular situation the criminal had already posted dozens of bogus products for sale on eBay.

No individual, law enforcement agency or government is any match for these criminals.

Very few are ever apprehended, and when they are, they can afford the best legal defense money can buy. Many openly admit to maintaining installations in other countries beyond detection of U.S. authorities -- and boast they can have new installations up and running within hours. They are highly successful. Protecting yourself properly can prevent you from adding to that success.

BUILDING A PASSWORD

- ❖ NEVER use a word found in ANY dictionary, nor combinations NEVER use a street, pet, child, relative or other "term" found in any language
- ❖ NEVER use "human readable" phrases of text (If it makes sense, they'll find it.)
- ❖ NEVER use your name or part of your name or phone number NEVER mix or merge passwords into a "new" password
- ❖ NEVER use the same password more than once
- ❖ NEVER use less than 8 characters -- 12 or more are better if the entry field allows it

Remember that NO password under 256 characters is 100% safe.

ALWAYS use combinations of upper and lower case letters mixed with numbers EXAMPLE: x9F32sS7riW5

CHANGE passwords frequently - at least once a year - monthly is best.

APPLY THE ABOVE RULES to ANY situation where a "password" is used. ... any financial account ... email accounts ... ISP and Dial-up accounts (like AOL or Earthlink) ... any online web site ... Home security systems ... Cell phones (Remember spammers now use hijacked cell phones for spamming)

AVOID situations where passwords are required. Ask yourself if you really need to join, subscribe, or participate in any activity where they ask you to set up a password.

Alerts have recently been posted of a renewed surge of criminals cracking into financial services, auction services and other sources of easy personal or financial information.

Identity theft is quick and easy once a password or account is cracked.

But Identity theft can also begin with * a cookie from a web site, * a careless post in chat room, * responding to spam * following a link in spam

Be vigilant with your passwords and accounts. Be vigilant with your online behavior and associations. Never ever underestimate the cross-referencing powers of the crime industry.

ALL people young and old need to understand this -- most particularly young people (who think they're invincible), the elderly (trusting and inexperienced in technology), the disadvantaged (searching for an easy way out). New, unskilled cable, DSL or wireless users are most at risk.

This victim had to cancel charge card accounts, and any online account the card was used for.

This victim had to delete an eBay account, and wipe a paypal account clean. And that's just the beginning.

Protect yourself at all times, and share this message with others. If you are in a position to disseminate this message to a larger audience, please do so.

Go to: <http://www.ftc.gov/> to learn more, or to report any suspicious online activity.

Join a local computer user group or club, and get educated. Build a network of knowledgeable friends or associates whom you can turn to with questions and help.

Protect yourself at all times.

Fred