

Hacking: What You Need To Know

hacking_

Presented by
Keystone Computer Concepts



Before we get started:

From now on, when you view the PowerPoint presentation from any of our webinars, you'll be able to read our notes for each slide. Let me show you how that works.



What is the definition of “hacker?”

A hacker is a person who looks for and exploits weaknesses in computer systems, computer software and computer networks. Hackers are often referred to as white hats.



What is the definition of “cracker?”

A cracker is a hacker who uses his or her abilities in a negative manner. Crackers are often referred to as black hats.

But really...

You rarely hear the term “cracker” outside of the IT community. Most non-computer media organizations refer to both white hats and black hats as “hackers.”



Why do crackers do what they do?

- 1) Profit
- 2) Bragging rights
- 3) Political statements
- 4) Payback
- 5) For fun
- 6) Because they can



What are the most common ways crackers cause problems?

- 1) By exploiting weak passwords.
- 2) Through social engineering.
- 3) By taking advantage of computers which don't have the latest updates.
- 4) By intercepting keystrokes on unprotected Wi-Fi networks.
- 5) Through keystroke-capturing software placed on a user's computer.



Misconceptions about cracking.

- 1) “I don’t have anything important on my computer; they won’t bother me.”
- 2) “I don’t do anything financial online so I don’t have to worry.”
- 3) “I’m too smart to fall for a cracker’s social engineering tricks.”
- 4) “I don’t go to gambling or porn sites where bad software is usually found so I’m okay.”
- 5) “This is too much. I should just throw my computer away and never go online again.”



What are ways to prevent a cracker from affecting me?

1) Exploiting weak passwords.

- 1) Use strong passwords. (See our blog post: <http://www.4kcc.com/blog2/?p=222>)
- 2) Change passwords from time to time.
- 3) Don't use the same password for everything.
- 4) Don't write your password where others can see or easily access it.



What are ways to prevent a cracker from affecting me?

2) Through social engineering.

- 1) Don't respond to emails, snail mail or phone calls which try to use fear, panic or deadlines to get you to give up personal information, buy a service or allow a stranger onto your computer.
- 2) Remember that NO financial institution will email you and ask you to click on a link to validate personal info.



What are ways to prevent a cracker from affecting me?

3) By taking advantage of computers which don't have the latest updates.

1) Keep your computer up-to-date including Windows or Apple updates, Adobe Air, Adobe Flash, Adobe Reader, Java, iTunes, QuickTime.



What are ways to prevent a cracker from affecting me?

3) By taking advantage of computers which don't have the latest updates.

2) If you are a Remote Technical Support customer, be sure to log in for the Quarterly Updates and log in if there's an update popping up and you're not sure if it's legitimate.

3) Read our blog for important information regarding updates.



What are ways to prevent a cracker from affecting me?

- 4) *By intercepting keystrokes on unprotected Wi-Fi networks.*
- 1) Never, ever, access financial sites when your computer is connected via a non-secure wireless network or a wireless network where everyone has the same password to gain access.

What are ways to prevent a cracker from affecting me?

5) Through keystroke-capturing software placed on a user's computer.

- 1) Keep your anti-virus up-to-date.
- 2) Don't let strangers on your computer – remotely or in person.
- 3) Be leery of plugging USB drives into your computer – drives given to you by strangers (such as classmates, library users, etc.)

What are ways to prevent a cracker from affecting me?

5) Through keystroke-capturing software placed on a user's computer.

4) Stay off of high-risk sites. Examples: gambling sites, porn sites, game sites from companies you never heard of, hacker sites and sites that offer well-known, expensive software for cheap or free.



What are ways to prevent a cracker from affecting me?

5) Through keystroke-capturing software placed on a user's computer.

5) Be leery of P2P connections (Napster, etc.)

6) Remember that Instant Messaging is also P2P and carries the same risks.

Things to Remember:

- 1) If given access and enough time, a hacker/cracker can get into your computer/email account.
- 2) Your job is to make it so difficult for someone to get into your “stuff” that he or she will move on to the next victim.

Our Final February Webinar

Tuesday, February 26, 2013 * 2:00 p.m.
Understanding Word Processing Programs

Our March Seminar

Saturday, March 9, 2013

10:00 a.m.-12 Noon

If You're Lucky Enough To Be Irish

We'll be covering videos - from your camera to email, to DVD and to YouTube.



All Day Word Class

Saturday, April 6, 2013

9:00 a.m.-4:00 p.m.



- At our home.
- We'll provide lunch.
- Minimum of 5 people, maximum of 10.
- Bring your own laptop (we have some loaners if you don't have a laptop)
- We'll cover tons of ways to make Word work better for you.
- Cost is \$60 per person.
- Register today!