Protecting your personal information online

By Roberto Caprio
14 Jul 2014

Identity theft and credit card fraud have reached epidemic proportions. You can scarcely go a day without reading a newspaper story about a major company losing thousands of customers' records. Hackers use a variety of methods in order to compromise and steal your information. Learn about some common hacking techniques and how to protect yourself.

Hacking techniques

Hacking takes patience, know-how, and an understanding of how websites and browsers work. Hackers can choose from several types of attacks when they plan to steal your personal data.

Phishing is one of the most common ways in which hackers gain access to personal information. Fraudulent, yet official-seeming, emails are sent to a recipient. The emails generally urge the recipient to enter his user name and password in the hope that the recipient will be tricked. Afterwards, the hacker uses this information to compromise the account.

SQL injection is another common type of attack. SQL injection takes advantage of poorly created queries by injecting commands into code that is sent to the backend database. Big companies, such as Macy's and Adobe, have fallen victim to SQL injection hacks.

Keyloggers is another type of common attack. These small programs run hidden in the background on a computer, completely invisible to the user. Keyloggers systematically record every keystroke made by the user and send the information to the hacker. Hackers then filter through the keystrokes and extract login credentials and personal information.

How can you protect yourself?

Protecting yourself is more about mitigating the damage from a compromised account rather than preventing any given

attack.

One of your best defences is to create unique passwords for each site. You can't control if a website is going to be compromised. However, you can prevent the information gained from being used to access additional accounts. Using a unique password for each online account prevents an attacker from compromising all your accounts with a single attack.

It's important to use a unique password for your email. If a hacker learns your email password he can easily reset the passwords on any of your linked accounts, possibly even gaining access to your financial accounts.

Another important step in protecting your information is enabling two-step verification. Two-step verification is becoming increasingly common for financial institutions. HSBC, the Bank of America and others are looking to this technology as a way to protect their account holders. Financial institutions aren't the only ones looking to protect their users though.

For example, Google has a two-step verification option. You enter your user name and password on a new computer and Google sends a security pin to your phone. You then enter this pin to log in. This process secures your Google account from third-party access, protecting not just your email, but also everything across the Google platform.

To defend against keyloggers, install an anti-spyware application. Dial a Nerd recommends Eset Nod 32. There is never a guarantee of 100% protection, but in the vast majority of cases Est Nod 32 will detect and quarantine software-based keyloggers. Then, it will disable or purge them.

Finally, be cautious of any emails with red flags, such as those that request you to login and verify your information, or reset your password. Even if the email "from address" looks correct, and the link or URL appears legitimate, you cannot be sure. Contact the company directly to ask about the email.

Where to get help

Dial a Nerd provides IT support at all levels, from the home user to large corporate networks. Several companies make use of outsourced IT support provided by our experienced team and long-standing educational institutions make use of our IT services because we are specialised in assisting with their specific requirements. Contact one of our consultants for an assessment of your IT requirements or simply for advice on how to protect your online identity. Dial a Nerd offers specialised IT and network support services for business, schools and individuals.

ABOUT THE AUTHOR

Roberto Caprio is MD of Dial a Nerd

For more, visit: https://www.bizcommunity.com