National Cyber Security Awareness Month // Avoiding Online Hacker Attacks and Scams

DON'T FALL FOR IT.

October is National Cyber Security Month, and as a provider of cloud hosting services, SingleHop is dedicated to helping spread the word about how people can keep themselves, their families and their information safe online.

We Need Your Help.

We're asking you to inform your readers about this important topic by writing a blog post that contains:

+ Details about how hackers and scammers can get your information online
+ Ways that people can protect themselves

To help you help us, we've put together some useful information below.

HACKING METHODS

Online Scams

Scam attempts have gotten way more sophisticated than the stereotypical Nigerian Prince trick. The FBI's Internet Crime Complaint Center (ic3.gov) lists dozens of variations on email and online scams – from fraudulent automobile auctions to online dating schemes – in its annual Internet Crime Report. In 2013 alone, more than a quarter of a million complaints were submitted related to online scams. And if you think it only happens to older people, think again: One fifth of scam victims last year were younger than 30.

Phishing

One particularly nefarious form of online scam uses legitimate-looking websites to trick a victim into sharing their username, password, or other sensitive information. Phishers will design their sites to look exactly like the website of your bank, credit card issuer, or another financial institution. The hope is that you won't realize you're on the wrong site, and just punch in your password like you normally would. Then, they use it to log into your real accounts and transfer out your money.

Massive Data Breaches

The above methods are all aimed at getting information about individuals. However, there's a whole profusion of hackers who are looking for the big score. Recent hacks of Home Depot, Target, and other major retailers have led to millions of credit card numbers being compromised. Hackers turn around and sell these numbers on a black market website for anyone who might be willing to buy them.

STAYING PROTECTED

Vigilance

Look carefully at a website before giving any information, especially sensitive data like passwords, credit card numbers or Social Security numbers. Especially look out for slightly misspelled words or words that use unexpected characters, such as substituting a "0" (number) for an "O" (letter) – for example, H0ME DEPOT. If something looks even a little bit fishy, delete the email or close the site immediately.

Browser Bookmarks

Rather than clicking on links in emails, create bookmarks in your browser to commonly used sites, like your bank, insurance company, etc., and use those bookmarks every time you visit the site. That way, you know you're always going to the right website, rather than trusting in an email that could've been sent by anyone.

Two-factor Authentication

More and more sites (especially those of financial institutions) are using two-factor authentication. With such methods, after logging in with your password, the site will text or email you a single-use code that must be entered. Only the registered phone number or email address will receive the code, making it that much harder for hackers to gain unauthorized access to your accounts.

Protected Servers

Consumers may not have direct control over how companies store their information, but with larger and larger hacks occurring regularly, you have a right to demand that companies take more responsibility for securing your personal information. For example, SingleHop embeds security features into their dedicated servers at the physical access level all the way down to the network, server, application, and account levels. Close monitoring along with antivirus protection, application patching, private networking, and firewalls all work to ensure that company data is protected and isolated.

Final Instructions

While we hope you find the information in this guide useful, we want to hear your take on online security. Whether you use any of the thoughts above or choose to go in a completely different direction, please share the link to your post with us.

Thank you again for your participation. We truly believe your awareness and sharing of this information will help everyone stay just that much safer online.

SINGLEHOP®