A Hacker's Tips on Keeping Your Personal Data Safe

One big concern for all of us these days is online safety and protecting our personally identifiable information and credit card information.

Not only that, but clicking on a nefarious link on a website or in an e-mail can unleash a cyber attack on your computer with bots rifling through all of your files.

In addition to online scams, criminals are also calling people and asking for personal information.

Recently, an anonymous hacker who now writes a cyber security blog had these recommendations for individuals who want to protect themselves and their files when online.

Here's the techie's advice:

Check senders carefully. Cyber criminals will try to get you to click on a link in an e-mail by making it seem like it comes from an official source, like "auditor@irs.gov." If in doubt, don't click on any links and call the agency using information from 411 or other legitimate sources.

Don't follow links to a site that's going to ask for secure information, such as a password. "If I want to raid your bank account, or do other harm, one way I can do it is to send you an official-looking e-mail with a link to your bank, asking you to log into your account for some reason," the hacker writes. If you go to the criminal's site, they will then obtain your log-in information and have access to your bank account.

Verify that the visual link and the actual link match. For instance, let's say the link is "PETA. org." But if you move your cursor over the link without clicking, most browsers will then show you the real link, either near the cursor, or at the lower-left corner of the window. If you see something like "PETA.smurfit.org" or "PETA.ru," or anything else that doesn't exactly match, it's likely they're trying to dupe you.

Don't automatically grant access for all programs. If you download a new game online and it asks you to enter the system manager password, you may be right to be suspicious as a game would not need system-level access.

Use unique passwords. If you are using a new site that requires a password, use a unique password, and one that can't be found in a dictionary. In other words, don't reuse a password from another site. This way, if the site is compromised and they get your unique password, they won't be able to access other online accounts of yours.

When a website asks security questions, give ridiculous answers. For instance, if a site asks which high school you went to, don't use the name of your real school. A dedicated hacker can find out where you went to high school. Instead, you might want to write something like "cuddly panda" or "fuchsia."

Ignore spam e-mail. You can often tell that e-mail is spam before opening it. Look at the "From" address. Do you know anybody named "Special Offer?" If the subject is odd, like "Donald Trump says he has a big brain, here's why," it's likely spam and should be avoided.

Set your e-mail reader so that it does not load images automatically or follow links automatically. For instance, if a scammer includes an image, allowing it to load can send the image ID to another server that then gains access to your system. Before you allow the browser to load images, check that every image name is generic. v

*This material was created by Insurance Newsletters and authorized for use by Brown & Stromecki Agency

###