Binary Tat Cat says... Don't do that!

Author : Cat

Date : February 2, 2016

Hold on a minute. Before you post that image, blog or tweet, consider the content. If it breaks even one of these rules, think really hard about putting it out there!

DO NOT....

Send a picture to someone via email/snapchat/instagram that you wouldn’t want your boss, principal, or grandma to see!

Sure you are sending them to your good friend or significant other. But what happens when that person is no longer your BFF? Or maybe their phone gets nabbed by someone with less morals.

The online proof: There are many sites that allow people to submit naked photos of their exes. I have taken down the links because they are NSFW (Not Safe for Work) and a breach of privacy.

Post personal information that is not readily available

Think about the last time you had to recover a password online. Was the question: Pet's name, childhood street, kid's birthday or mother’s maiden name? Make sure that kind of information stays private and don't use it for the actual passwords.

The online proof: Here are the most common and hackable passwords.

Announce when you are going away

Yes, your friends are excited that you only have 3 more days until you leave for Hawaii! But so is the guy that has been staking out your house. You think you used Foursquare to get a discount at a restaurant. Someone else used it to know you were not at work.

The online proof: The website PleaseRobMe.com is a collection of data from various social sites that tells you who is away. This one is for educational purposes but there are less savoury ones.

Underestimate what your device or computer already knows about you

All online content is tagged with metadata which contains anything from the timestamp it was created to the location. You cannot see the metadata when you post but simple free software can pull it for someone else. Be wary of geotagging on mobile devices, which marks where you took the photo.

The online proof: Check out I know where your cat lives for a series of random cat pictures pulled off the internet and then tagged to the location where they were taken using hidden metadata.

Forget to set your privacy settings

Not only should you check your settings at the outset but you should recheck them frequently. Facebook, for example, uses an ‘opt out’ policy which means that by default you are sharing more information until you go in and update those settings. Follow us on Twitter or Facebook or join our mailing list to get those updates sent to you.

The online proof: Here is a fantastic infographic that shows how Facebook privacy settings have changed and what data is now available if you haven't updated them.

Post negative comments about your workplace or coworkers

Even if your boss or coworkers are not able to see your comment, a future employer could see that comment and reconsider hiring you later. Even with privacy settings set, you are at the mercy of our online friends not to share.

The online proof: Here are examples of people actually fired due to their social post.

Post photos of your friends that break the first rule

It is a great photo of you. So what if your friend is doing something in the background that would tarnish their reputation? If you tag them, your friend can remove the tag, but unless the photo violates terms and conditions (allowing a site to pull it down) only you control the permissions on that photo. Put yourself in their shoes (and hope they would do the same). This goes double for pictures of underage kids. If the child is under 18, you technically need the parents permission to post it.

The online proof: This article talks about the inability to remove someone else's photo.

Use the same password for every account

I know it is a pain to remember different passwords for all of your sites but it is an even bigger pain if someone hacks in to one of your accounts. Are you using the same password for your social networks, banking, or online shopping? If a hacker finds just one instance of your password then they will now have access to everything.

The online proof: Here is just one example where hackers breached the Adobe database and were able to access users' Facebook accounts because the email-password combinations were the same.

Do you have a great tip that you don’t see here?

Post it in the comments!

OR

Contact Us and let us know!