Data Exfiltration

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

Data exfiltration is the unauthorized transfer of data from a computer or other device. It can be conducted manually via physical access to a computer or through malicious programming on the internet or a network.

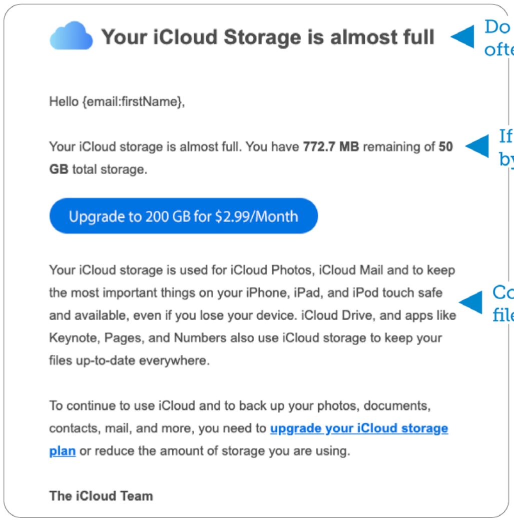
Attacks are typically targeted, with the objective of gaining access to a network or machine to locate and copy specific data. In addition to malicious attacks, human error can also play a role in data loss.

Cyberattacks often begin with phishing emails. Signs include:

- A sender address you don't recognize or doesn't make sense.
- An empty 'To' address field or one with names you don't know.
- A send date or time that falls outside normal business hours.
- A heightened sense of urgency or alarm.
- Promises of rewards or threats if you do or don't act.

If you suspect anything suspicious, alert your IT team immediately as it could be part of a larger attack. By recognizing the clues in the sample email provided you can avoid these attacks.

Example



Your iCloud Storage is almost full

Hello {email:firstName},

Your iCloud storage is almost full. You have **772.7 MB** remaining of **50 GB** total storage.

Upgrade to 200 GB for $2.99/Month

Your iCloud storage is used for iCloud Photos, iCloud Mail and to keep the most important things on your iPhone, iPad, and iPod touch safe and available, even if you lose your device. iCloud Drive, and apps like Keynote, Pages, and Numbers also use iCloud storage to keep your files up-to-date everywhere.

To continue to use iCloud and to back up your photos, documents, contacts, mail, and more, you need to **upgrade your iCloud storage plan** or reduce the amount of storage you are using.

The iCloud Team

Do you even have an iCloud account? Scammers will often make claims like this to get you to react.

If you're not sure if this is the case, check your storage by visiting the actual source, not by clicking the link.

Copy is designed to create anxiety over losing important files and get you to act.

Overall, this is a sophisticated phish, but being skeptical and keeping your emotions in check can help you avoid falling for it.