East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Friday 26 June 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

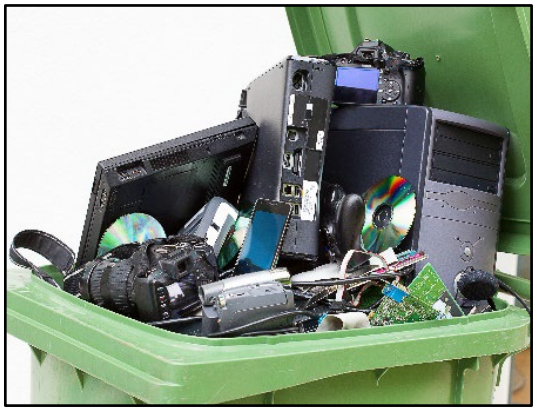
If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is: Erasing data

We have probably all experienced that moment of dread after accidentally deleting a file, document or email, followed by the relief of going to the recycle bin or deleted items folder and recovering the item. Even when the items have been permanently deleted from the recycle bin and appear to be gone forever, they are still on the system.

Easily available recovery software can search out these ghost files and restore them.

The bad news is that when digital devices are sold, recycled or even sent to the tip, the data is still there and recoverable.



Few of us stop to think of the amount of sensitive data that we store on our digital devices; computers, mobiles, cameras, USB drives, printers and fax machines.

Examples of personal data that are processed and stored by these devices include; bank information, passwords, medical data, job applications, personal photos, contact lists and tax returns.

Deleting files, reformatting storage devices or even using the 'back to factory settings' does not remove the data! This information is vulnerable to unauthorised or malicious access.

The term 'dumpster diving', where criminals sift through waste to commit identity theft, applies to technology just as much as it does for un-shredded documents.

Examples of data breaches

On a printer used by a New York construction company, CBS News found "design plans for a building near Ground Zero in Manhattan; 95 pages of pay stubs with names, addresses and social security numbers; and $40,000 in copied checks."

A machine, once used by Affinity Health Plan, a New York insurance company, contained "300 pages of individual medical records." These records included "everything from drug prescriptions, to blood test results, to a cancer diagnosis."

East Midlands Special Operations Unit

What can I do?

- **Overwriting:** A process of preparing media for reuse by writing random 0s or 1s over the entire storage device. Overwriting data uses multiple passes and there are software products that can do this. The more overwrites the better. However, data may still be retrievable, especially on hard drives which have 'bad sectors'. Many SSD devices include 'secure erase' but this is not fool proof and may still leave the data recoverable.
- **Degaussing:** This generates a heavy magnetic field to corrupt the data on magnetic media beyond the point of retrieval. This works reasonably well for tapes, floppy disks and some hard drives, but there is no guarantee. Degaussing does not work on CDs, DVDs or SSDs.
- **Destruction:** The most secure method of sanitising media and includes; incineration, crushing, shredding, disintegration and dissolving using caustic or acidic chemicals. Like degaussing, this often requires the services of an accredited disposal company and can be quite expensive, although this can be free, or discounted for schools and charities. Reputable companies will issue a certificate of disposal which provides a guarantee that the data is irretrievable.

The unique challenges of Cloud Computing

In Cloud Computing, the cloud vendor will not destroy hardware when a customer leaves. Instead, they are repurposed for other users. The data is also in a constant state of flux within a pool of resources and overwriting of media, to sanitise it, is not common.

To ensure data is safe from unauthorised access in the cloud, an organisation must make sure that sensitive data is encrypted. When cloud services are no longer required, the keys to access this information are destroyed. The storage of encryption keys and their destruction (known as 'cryptographic erasure') must be carefully considered before moving into this type of environment.

Additional protection measures:

- Many devices are able to encrypt data as it is stored; adding an additional layer of security when devices are disposed of.
- Best practice dictates that if storage media is to be reused, subsequent data must be of the same sensitivity/classification as the original data. For example, a hard drive that stores 'Secret' data would not be downgraded to 'Unclassified'.
- Make sure that all digital devices, to be disposed of, are securely stored pending collection by a disposal company.

Hot topics

Security researchers have identified a campaign of unusual cyber-attacks with malicious documents attached to phishing emails. The document downloads a compromised image that contains malware hidden in its pixels, a technique called steganography.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).