DATA SECURITY E-BOOK:

10 TIPS FOR KEEPING YOUR DATA SECURE

EQUIPNET

equipnet.com/technology

DATA SECURITY E-BOOK:
10 TIPS FOR KEEPING YOUR DATA SECURE

one

Update your operating system and software.

You get a number of notifications on our desktop, laptops, smart phones and other devices asking you to stop what you are doing and commence the latest software and OS updates. This can be quite inconvenient while trying to get your work done, but its relevancy is quite important!

Although these updates may seem intrusive to your work, they are not only essential for your OS functionality, but many times, they contain vital security updates for your device as well.

Be sure to accommodate these software and OS updates as soon as possible to keep your computer and devices properly protected.

EQUIPNET

equipnet.com/technology

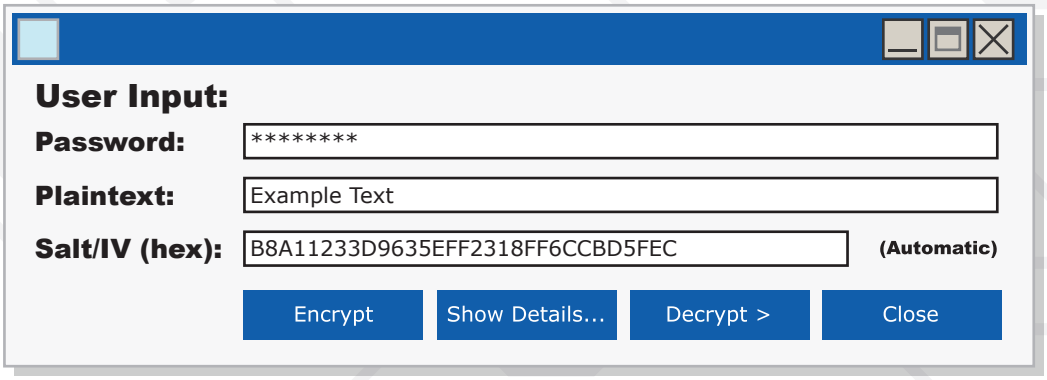
two

Encrypt sensitive data.

Encryption is one of the most effective means of data security, and involves converting your electronic data into a different form, known as ciphertext, which is only understood by authorized personnel.

Utilizing encryption tools ensures your data will remain unreadable and secure, even when invaded by malicious hackers. It is important to encrypt data that is transferred onto a storage device as well, in case your USB drive or device is misplaced or stolen.

Some free data encryption tools include VeraCrypt, AxCrypt, BitLocker and many others.



three

Utilize antivirus software.

Although it is known that antivirus software cannot protect against a number of threats, it is still an essential baseline for protecting your devices against common malware. There are many free and reputable antivirus tools available that will perform periodic virus scans and more.

Some common free antivirus software systems include AVG, Avast, Panda and BitDefender.

four

Change your passwords in the event of a data compromise or breach.

We hear about data breaches continuously, whether it be in large corporations or small family-owned businesses. In 2014 alone, over 1 billion records were breached, averaging about 32 breaches per second. Some of the largest data breach victims in recent years include Target, Home Depot, EBay, JP Morgan and many other well known corporations.

When you become aware of a data breach on a website or company you are associated with, your first and most essential step is to change your passwords for those accounts immediately. This ensures that your old credentials are counterproductive for the hackers.

five

Use different and complex passwords for each account you have.

Many individuals are guilty of using the same passwords for email accounts, online banking and social media profiles; what you don't realize is the trouble you could get into if one of your accounts is unfortunately hacked and your data is breached.

Many hackers will try logging into various accounts using the same login information they previously obtained. In other words, once that hacker gets into your Facebook account, they now have access to your PayPal, online banking information, email accounts and or any other account that that has the same password.

six

Monitor your online account activity.

Always remember, if it looks or seems suspicious, it probably is. Monitor your accounts regularly and if you notice anything different or unusual, be sure to notify the involved companies immediately. Monitoring your accounts regularly allows you to quickly identify potential breaches or compromises.

seven

Archive or delete unnecessary data.

Ridding your devices of old or obsolete data minimizes the amount of information available to a hacker and is a good habit for maintaining organization on your devices. As mentioned, when you transfer these files onto your storage device, be sure to encrypt your data. Such practices should be done especially for personal data, including bank statements, bills, health records and other confidential documents.

DATA SECURITY E-BOOK:

10 TIPS FOR KEEPING YOUR DATA SECURE

eight

Properly adjust your privacy settings.

With technology growing and becoming increasingly innovative, many of you have a number of different apps and online accounts downloaded onto your devices. It is essential to have the appropriate security and privacy settings implemented to ensure you are not allowing companies and/or individuals access to your private information.

EQUIPNET

equipnet.com/technology

nine

Free/unprotected Wi-Fi networks are not safe.

Free Wi-Fi is great and there's nothing like connecting to a free network and saving some gigabytes while at the mall, coffee shop or on vacation. Many neglect to be wary of these open networks and forget the associated risks, especially in high-traffic areas. Hackers use unprotected Wi-Fi networks to see what victims are available to them. If you are connected to an unprotected network, ensure that HTTPS – the secure version of HTTP – is enabled for any/all sites you visit.

DATA SECURITY E-BOOK:
10 TIPS FOR KEEPING YOUR DATA SECURE

ten

Become aware of phishing scams and avoid them.

Hackers become more innovative each day to try to convince you to hand away your personal information. A common phishing scam includes fraudulent emails that look like your average, every day email. These emails may appear as if they are coming from a trustworthy source, such as your bank, employer, etc. Once you click on a link within these email messages, it directs you to a spoofed website, some of which attempt to get you to give away your private data, such as your credit card number or password.

Learn to recognize these types of attacks by checking the sender information, domain names and the attachments and URLs included. Be sure to ask yourself if you even requested this type of message and review its relevancy.

As stated, if it looks or appears suspicious, it probably is.

EQUIPNET

equipnet.com/technology

DATA SECURITY E-BOOK:

10 TIPS FOR KEEPING YOUR DATA SECURE

LEARN MORE ABOUT KEEPING DATA SECURE WITH EQUIPNET

equipnet.com/technology
+1.781.401.8160
bschugar@equipnet.com
@EquipNet
linkedin.com/company/EquipNet
facebook.com/EquipNet

SOURCES

http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf
https://digitalguardian.com/blog/10-data-protection-tips-data-privacy-day-2015
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

EQUIPNET