East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

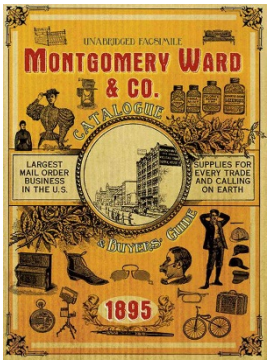
Monday 11 May 2020

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 'online shopping'



Distance retailing has its roots in 1870's Chicago. Aaron Montgomery Ward came up with the idea of a mail-order business, to supply goods to rural customers, who could purchase by mail and collect at the nearest train station. Ward's 240-page 1883 catalogue listed 10,000 items and created the slogan **"satisfaction guaranteed or your money back"**. In 1939 the Christmas promotional campaign created the character **"Rudolph, the Red-Nosed Reindeer"**.

In the early 90's Montgomery Ward were one of the first retailers to carry consumer products from IBM, Apple, Compaq, and Hewlett Packard, heralding the growth in home computing.

Today we find ourselves with computers in every home and retail giants such as Amazon selling thousands of products online. COVID-19 has further encouraged consumers to buy products online that they would normally buy in-store. During such times, it is important to remain cyber aware to avoid falling foul of online criminals.

Top tips

Stay up to date: Install the latest software and app updates. Information can be found on how to install updates from Apple, Microsoft and Google. Always use a verified trusted source for software updates and turn on automatic updates.

Secure online accounts with a good password: Use three random words. This makes the password extremely difficult to crack. It also acts as a 'pass phrase', which is easier to remember. Consider downloading a reputable password manager which will generate complex passwords and will auto-complete forms, make sure that the master password is complex.

Turn on two factor authentication (2FA): Where possible turn on two-factor authentication (2FA). This is a way to double check the identity of a person when logging in e.g. by sending a security code to a mobile phone. Cyber criminals in possession of a password can't access the account unless they have this "second factor".

Links in emails and texts: Emails or texts offering amazing deals may contain links to fake websites, designed to steal money and personal details. Not all links are bad, but it's good practice to check by typing the sellers' website address into the address bar of your browser or find the website through a search engine and only shop on sites that you trust.

East Midlands Special Operations Unit

Always check that the address bar shows 'https' and log out when done. The padlock sign means that the connection is encrypted, so personal information will reach the site without anyone else being able to read it, but it doesn't tell you who is at the other end of the connection. Use a credit card, as most major providers insure online purchases.

Form filling: There are details that an online store will need, such as address and bank details, be cautious if they ask for details not required for purchases. Only fill in the mandatory details on forms (usually marked with an asterisk*).

Hot topics

A new scam has been reported where the victim is contacted by someone purporting to be from Amazon, stating that their Prime account is changing from £7.99 a month to £79 each quarter. Amazon has confirmed this is a scam.

New HMRC-themed phishing scam reported. Recipients sent fake emails claiming the government has introduced a new tax refund programme due to COVID-19 and they are entitled to £179.21. Criminals are spoofing the email address of a genuine UK government brand (noreply@hm-revenue.gov.uk) to trick recipients. The email includes links to access the refund and information on how to protect from the virus. Links have been confirmed as malicious – infecting devices with malware and stealing personal information.

A new phishing attempt, claiming to be from a payroll admin department, asking staff to verify their email account for a new payroll directory and adjustments made to their pay. These emails display the subject line header "COVID-19/MAY PAYROLL BENEFITS" and recipients are asked to click on a link to provide details. This provides an opportunity to steal email logins, passwords, personal details and appear personalised with the recipient's email.

Emails claiming to provide information on how Greece avoided a COVID-19 lockdown have been seen with a link to view the article; which has been confirmed as malicious.

Webinar – Thursday 11th May 2020 @ 1400 – 1500 hrs

Topic: Security in the Cloud - A Guide for Small to Medium Sized Organisations

Join East Midlands Special Operations Unit, as they host a free Webinar on Cloud cyber security issues.

Cloud services are becoming a fundamental facet of doing business online. Metered services, rapid elasticity and improved IT security offer a one stop solution to all computing needs. Or do they?

Explore some of the key security issues surrounding the use of the cloud and how to make sure that your organisation stays cyber secure. - To register for this event click on the following link - places are limited.

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).