THE EASTERN CYBER RESILIENCE CENTRE

TOP TIPS FOR CYBER RESILIENCE

PASSWORDS

A strong password is one that's tricky to guess and includes a mix of uppercase and lowercase letters, numbers, and special characters. The NCSC recommend use three random words followed by punctuation to create a secure and separate password.

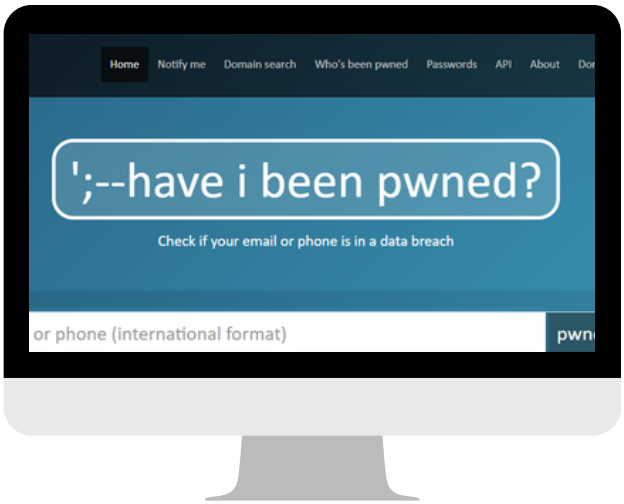
To find out more about passwords guidance, check out our Guidance | Eastern CRC (ecrcentre.co.uk).

WHAT'S NEXT?

1. See what passwords you and your staff have which have already appeared in data breaches and change them as soon as possible. Haveibeenpwned.com is a legit website where you can enter your email address and telephone number to see if your information has been captured in a data breach. You can also register your email address or domain and get notified if it appears in another breach.

2. Establish a clear password policy for staff and educate them about the importance of having strong and separate passwords. If you need some help with this, our affordable student services offer security awareness training. Feel free to book a chat to discuss this further.

3. If your staff have a lot of passwords to remember, consider getting an enterprise password manager so they only have to remember one and the password manager generates and remembers the rest – saying goodbye to reused passwords.



THE EASTERN CYBER RESILIENCE CENTRE

MULTI FACTOR AUTHENTICATION

Two Step Verification (2SV) and Multi Factor Authentication (MFA) play a vital role in safeguarding your systems, accounts, and devices. They offer an extra layer of protection by utilizing two or more methods to verify your identity.

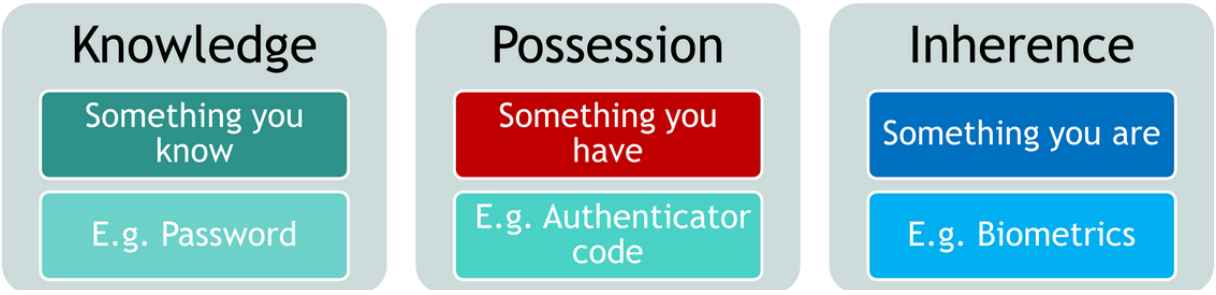
Even with strong passwords, if someone gets hold of your password, the security of your system is compromised.

However, by implementing 2SV or MFA, cybercriminals cannot gain access simply by cracking your password. They would also need your fingerprint, Face ID, or your mobile phone to authorize a login attempt using a mobile authenticator app.

WHAT'S NEXT?

Enable 2SV and MFA wherever you can, but especially on your emails and social media accounts to provide that last line of defence in a cyberattack.

Types of 2SV/MFA information:



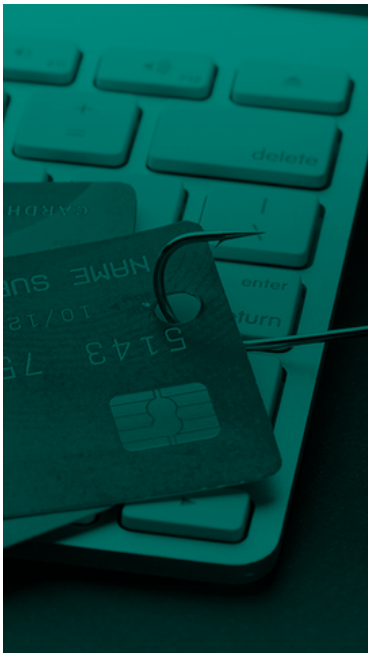
PHISHING ATTACKS

The most popular type of cyber-attack in 2022 was phishing attacks.

Phishing is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords

THE EASTERN CYBER RESILIENCE CENTRE

WHAT'S NEXT?



1. Educate your staff and volunteers about the risks and best practices for identifying and avoiding phishing scams. If you need some help with this, our affordable student services offer security awareness training.

2. Have a plan in place to deal with phishing attempts and successful attacks. Make sure your staff know how to report an attack and don't put barriers in place to reporting.

3. Make sure you report all phishing attacks to report@phishing.gov.uk. The NCSC will the actively seek to disrupt the criminals sending these messages, protecting you from them as well as the wider community.

KEEPING YOUR DEVICES UP TO DATE

Device manufacturers and app developers regularly roll out software updates that come with exciting new features, bug fixes, and performance enhancements. But that's not all—they also pack in essential security patches and new security features that you shouldn't ignore.

Why are these patches so important? Well, they're designed to fix any known weaknesses in the products that can be exploited by attackers. By installing these patches, you're closing the door on potential threats and making it harder for attackers to mess with your devices.

WHAT'S NEXT?

While many devices and apps can update themselves automatically, there might be times when they need a little nudge from you.

So, make sure to keep an eye out for updates and lend a helping hand if needed. It's all about keeping your devices secure and running smoothly.

THE EASTERN CYBER RESILIENCE CENTRE

JOIN OUR COMMUNITY

Join our community as one of our growing numbers of free core members. You will be supported through implementing the changes you need to make to protect your organisation.

Core members receive regular updates which include the latest guidance, news, and security updates. Plus, you will get access to our brilliant Cyber Security and Resilience services.

We are already working closely with hundreds of organisations across the seven counties to help them tackle the continually changing cyber threats that they face. So come and join our community as free members and let us help you protect your organisations from the ever presents threats out there in the cyber-verse. Feel free to book a chat to discuss this further.

REPORT A CYBER ATTACK

Reporting a live cyber-attack 24/7

If you are a business, charity or other organisation which is currently suffering a live cyber-attack (in progress), please call Action Fraud on 0300 123 2040 immediately. This service is available 24 hours a day, 7 days a week.

Reporting a cyber-attack which isn't ongoing

Please report online to Action Fraud, the UK's national reporting centre for fraud and cybercrime. You can report cybercrime online at any time using the online reporting tool, which will guide you through simple questions to identify what has happened. Action Fraud advisors can also provide the help, support, and advice you may need.

Report a phishing attack

If you suspect a phishing attack, please report it to the Suspicious Email Reporting Services (SERS) set up by the NCSC at: report@phishing.gov.uk
Text messages can be forwarded to 7726