

# Top tips for preventing cybersecurity attacks

We are actively working to protect our business and our supply chain partners from cyber criminals. We want to work with you to help keep ourselves and our supply chain “cyber” safe. This resource contains information on key cyber security topics, as well as guidance on best practice.

## What could be put at risk?

Money, IT equipment, websites, payment systems, personal/confidential information and reputation are all at risk from cyber criminals, but it's not just businesses that are targeted. On a personal level, this could mean your bank account, your sensitive personal data and everything you connect to the internet is at risk.

## Contents

- **Phishing:** The attempt to steal sensitive information such as passwords and credit card details.
- **Passwords:** This is your primary mechanism to prove your identity when using the internet, knowing what is a good vs. bad password is essential to keeping attackers away from your information.
- **Protecting our assets:** How to keep your devices and documents safe and secure to reduce the chance of an attacker using them to access your information.
- **Out and about:** What you need to consider to be safe when working away from the office or home.
- **Email:** What to watch out for in emails that could be tricking you into doing something you were not expecting.

## What are we doing about it?

We are actively working to protect our business and our supply chain partners from cyber criminals. We have modern technology to help in this fight, but the most frequent and successful attacks come from social engineering. We can't protect everything, so we need everyone to be vigilant. We've summarised some key topics and ask that you please share this information with your teams. We hope you find this resource useful. We look forward to working together to keep ourselves and our supply chain cyber safe.

## Phishing



Phishing is an example of a social engineering technique being used to deceive users. It's typically carried out by email, phone calls and text messages and will trick you into revealing your personal information. This information is then used against you and, at worst, this could mean your email account is open to someone else and/or fraud is committed leaving you out of pocket or in debt.

Spotting the signs of phishing will help you take appropriate action.




## How to spot Phishing attacks

- Watch out for emails, calls or text messages with a sense of importance or urgency
- Is the sender making requests for personal information, a payment or signature?
- Does the email seem rather vague in detail, for example, are the recipients formally addressed or does the conversation start with 'Hello?'
- Are there unfamiliar links in messages? If in doubt hover your mouse over to see the destination but **do not click!**
- Do you recognise the sender's email or text message style and/or signature?
- Does the sender have a name you recognise and, if so, would they typically send a request in this way?

## Dos

-  **Do** change your password if you think you've entered or supplied any personal or logon details as a result of a phishing attack. If you use that password on any other systems, these must be changed too
-  **Do** delete or report suspicious emails or messages to your security team

## Don'ts

-  **Don't** click links or open attachments that you don't recognise
-  **Don't** submit your credentials and any personal information on links and websites that you don't recognise
-  **Don't** reply to emails or text messages you know or suspect to be phishing

## Passwords

Your account password is a very attractive target for cyber criminals. Many social engineering and phishing attacks will trick you into revealing your password. Fake websites that look just like your webmail, file downloads and IT support services are all examples of ways the attacker will trick you into entering and gaining your password. In some cases, an attacker might try or guess your password based on information they know about you from hacks against other systems. Having good, strong passwords that are unique for each system you use are essential to prevent them from being successful.

### What is a good password?

A good way to create a strong and memorable password is to use a passphrase; three random words mixed with numbers and/or symbols, for example:





3redhousemonkeys27!




That password would take about 314 years to crack.

### How you can protect your logon details





- Always use unique passwords for your accounts
- Be aware of social engineering techniques that utilise impersonation to trick you into giving away credentials
- See if your password has already been stolen by using [www.haveibeenpwned.com](http://www.haveibeenpwned.com)

## Dos

-  **Do** use Multi-Factor Authentication (MFA or sometimes known as 2FA) whenever possible. MFA adds another layer of security to any account and in some cases may replace a password altogether
-  **Do** choose words that are memorable but avoid those which might be easy to guess, such as 'onetwothree'
-  **Do** use a combination of uppercase and lowercase letters, symbols and numbers
-  **Do** make sure your passwords are at least eight characters long. The more characters and symbols your passwords contain, the more difficult they are to guess

-  **Do** make use of a Password Manager to securely store passwords BUT remember to use a strong password to protect them
-  **Do** change your password if you suspect it has been stolen
-  **Do** log out of websites and devices when you are finished using them

## Don'ts




-  **Don't** use commonly used passwords such as 123456, the word "password," "qwerty", "111111", or a word like, "monkey"
-  **Don't** use your name, a family member or your pet's name. Avoid using phone numbers, addresses and birthdays
-  **Try not to** use the same password across multiple websites, systems and/or applications
-  **Don't** write down or share your passwords or let anyone see you log into devices or websites

## Protecting our assets



Items of value such as laptops, mobile phones and documents/ print-outs that contain personal and/or business data are all valuable to criminals. Not only do they contain information about you, they can be sold for a quick profit perhaps to someone who has more interest in the data they hold than the device itself.

### How you can protect your logon details

## Dos

-  **Do** ensure your laptop/tablet and phone are protected with a password or PIN (or fingerprint if supported)
-  **Do** run anti-virus software if your device supports it and check that it is up to date
-  **Do** make sure the printed information is secure

## Don'ts

-  **Don't** download software or music that you know to be illegal
-  **Don't** plug in or connect to devices that are not trusted (such as external USB keys, connecting to unfamiliar WiFi hotspots etc.)






## Out and about


When travelling with your laptop/tablet and/or phone be aware of people around you who might spot such devices as quick and easy items to steal.

## How to keep safe when carrying out work in public spaces

### Dos

-  **Do** be aware of who can see your screen while working as they might see sensitive information
-  **Do** only connect to trusted WiFi networks
- Do** keep assets secure and out of sight when not in use especially when left in a vehicle
-  **Do** keep assets in a carry-on bag and not in luggage as they might get damaged or lost/stolen

### Don'ts

-  **Don't** leave assets unattended even if you will be away for a short time

### Email

Email is one of the easier targets for hackers and phishing. The more public your email address is, the more likely it will be targeted.

## What to consider when using email

- Am I expecting an email from this sender?
- Does the grammar and spelling look correct?
- Does the display name match the actual sender's address?
- Is what I'm being asked reasonable or is additional pressure being applied by indicating there is limited time to resolve?
- Email should not be considered secure. You should protect sensitive data by encrypting it or using alternate ways to deliver it (OneDrive for example)
- Does your email service offer any security services such as anti-virus and anti-phishing protection? While these will never be 100% effective, they will reduce the amount of unwanted emails

Keep an eye out for regular news articles on cyber security. Please visit:

[Getsafeonline](#)

[National Cyber Security Centre](#)

If you work for Balfour Beatty and wish to report a suspicious email, call, or attachment, please email: [itsecurity@balfourbeatty.com](mailto:itsecurity@balfourbeatty.com)

If you are part of our supply chain and wish to report an incident which may affect us, please reach out to your Balfour Beatty contact who will raise the issue on your behalf.

