At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by

NOS National Online Safety®

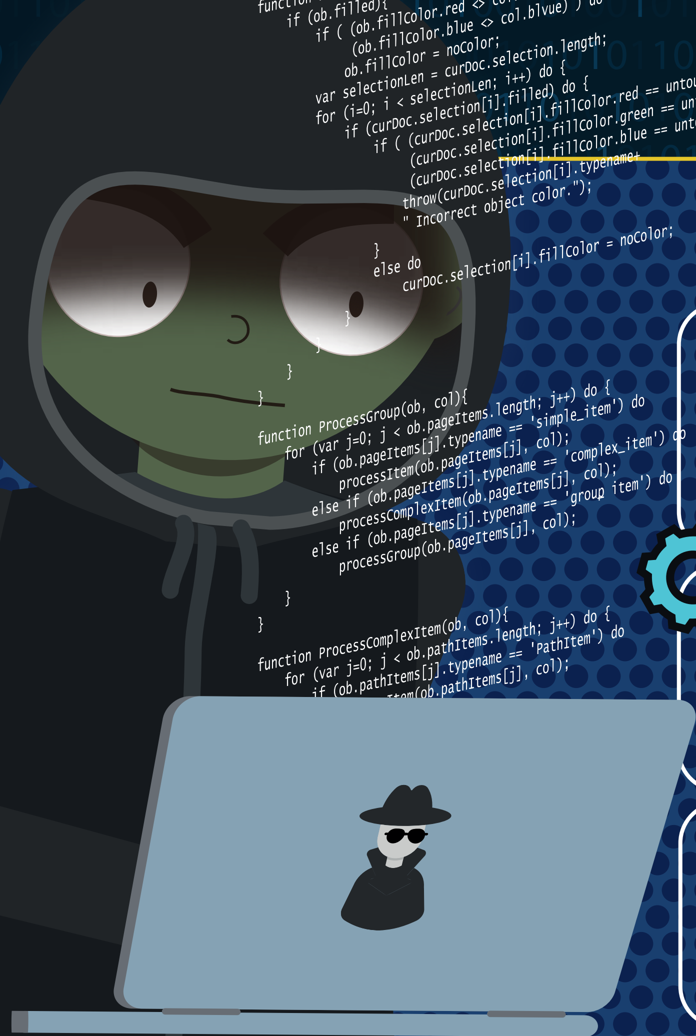
www.nationalonlinesafety.com

What you need to know about... HACKING

What are they?

'Hacking'

Hacking is the unauthorised attempt to exploit a computer system or network. There are different types of hackers who are usually categorised under 'hats'. White hat hackers are known as ethical hackers and have no intent to cause harm, but rather will penetrate a system to identify weaknesses. Black hat hackers or Crackers are those who intentionally hack to gain unauthorised access to harm or steal sensitive information. Grey hat hackers act more for fun and exploit security weaknesses in computer systems to raise awareness of issues for recognition, political awareness, or financial reward.



```
r untouchColor = new RGBColor(
ar curDoc = core.activeDocument;
if (curDoc.selection.length > 0)
    var uncolPaths = curDoc.selection;

if (uncolPaths.length>0) do {
    for (i=0; i < uncolPaths.length; i++) do {
        if (uncolPaths[i].typeName == "group_item") do
            ProcessGroup(uncolPaths[i], untouchColor);
        else if (uncolPaths[i].typeName == "complex_item") do
            ProcessComplexItem(uncolPaths[i], untouchColor);
        else do
            ProcessItem(uncolPaths[i], untouchColor);

    }
}
function ProcessItem(ob, col){
    if (ob.filled){
        if ( (ob.fillColor.red <> col.red) or (ob.fillColor.green <> col.green) or
            (ob.fillColor.blue <> col.blvue) ) do
            ob.fillColor = noColor;
        var selectionLen = curDoc.selection.length;
        for (i=0; i < selectionLen; i++) do {
            if (curDoc.selection[i].filled) do {
                if ( (curDoc.selection[i].fillColor.red == untouchColo
                    (curDoc.selection[i].fillColor.green == untouchCol
                    (curDoc.selection[i].fillColor.blue == untouchColor.
                    throw(curDoc.selection[i].typename+
                    " Incorrect object color.");

                }
                else do
                    curDoc.selection[i].fillColor = noColor;

            }
        }
    }
}
function ProcessGroup(ob, col){
    for (var j=0; j < ob.pageItems.length; j++) do {
        if (ob.pageItems[j].typename == 'simple_item') do
            processItem(ob.pageItems[j], col);
        else if (ob.pageItems[j].typename == 'complex_item') do
            processComplexItem(ob.pageItems[j], col);
        else if (ob.pageItems[j].typename == 'group item') do
            processGroup(ob.pageItems[j], col);

    }
}
function ProcessComplexItem(ob, col){
    for (var j=0; j < ob.pathItems.length; j++) do {
        if (ob.pathItems[j].typename == 'PathItem') do
            [illegible]Item(ob.pathItems[j], col);
```

Know the Risks

It's Illegal

Hacking is often portrayed in the media as dark, dangerous and cool. However, young people attempting to hack are often unaware that they are actually breaking the law. It is a criminal offence to access or modify data stored on a computer system without permission which is often punishable by law and could lead to a criminal record.

Theft of Personal Data

Cyber criminals collect information in a variety of ways and will try to entice children to an attractive website through offers of free media or products. They will often hide malware in downloadable content which can take over your computer, steal personal data and pass it on to third parties. This can lead to financial and reputational damage, embarrassment, blackmail or even identity theft.

Inappropriate Content

If a child is using an unsecure network, free WiFi or hasn't implemented any necessary security measures, they could leave themselves open to being hijacked by other users. This could leave them open to being sent or exposed to inappropriate images or videos, especially via social media platforms or communication apps.

18+

Safety Tips

Talk about the risks

Encourage discussion with children about what hacking is and what the consequences of being hacked are, as well as those risks if they were to become involved in hacking themselves. Discuss the legalities and the dangers of not keeping accounts and passwords secure.

Be security aware

Talk to children about being security aware. Advise them to seek your help when filling out online forms and make sure they know what to keep private when filling in online profiles such as their date of birth, phone numbers and addresses. Make sure children know the risks of connecting to open/free Wi-Fi.

Tighten protection

Make sure that you have implemented necessary security measures across all devices and apps your child uses. Use passwords that are made-up of at least 8 characters consisting of symbols, numbers, uppercase and lowercase letters. Create different passwords for different accounts and use two-factor authentication where possible. Turn off browser pop-ups and location services in apps when not in use and make sure your anti-virus software is up to date.

Further Guidance

Provide support

Try to make sure that child know that they can feel comfortable talking to you. If a child's account has been hacked and they have suffered embarrassment or loss of private information, they may become withdrawn, secretive or emotional so it's important that they know that you will be there to help and can offer them support and advice to help rectify the situation.

Change security controls

If you suspect that a child's account has been hacked or compromised, disable it, change passwords for other accounts that may be linked to it and use a password manager to increase the level of security.. If you believe a device has been hacked, update and run your anti-virus software. You might also need to wipe the device and re-install everything.

Seek further help

If you notice that a child is starting to show a deep interest in hacking activities or mentions the dark web or TOR browsers, have a conversation with them about the laws they may be breaking and the possible dangerous consequences. Seek advice from local organisations who may have more specialist knowledge and can provide further guidance.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

afety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.09.2020