Sian
Hi there – great news! I've just received an email and it turns out I'm a millionaire!!!
According to this email, I've won the lottery: I'm rich, rich beyond my wildest dreams! All I
have to do is send them my bank details and they will put the money in my account. Now,
what shall I spend my millions on? The funny thing is, I don't even play the lottery! Oh, wait
a minute…

Did you see the mistake I made there? I nearly gave my bank details to a stranger online. I
could have lost all my money! It just shows how important it is to be careful online both in
your personal life and as a distance learner. So that's what we are going to look at today:
safety & security. As a distance learner, you will be using digital resources and platforms as
part of your studies. That means you need to be safe and secure.

So what does it mean to be safe and secure digitally? Well, it can include: Making sure your
digital accounts are secured with strong passwords. Keeping your personal details secret so
people online don't know everything about you. And being aware of hoaxes, scams and
tricks so you don't fall for the same kind of trick that I nearly did.

There are many reasons why we need to be safe and secure when we are in the digital
world. As a distance learner, you need to be careful not to reveal personal information
about yourself or anyone else online. You don't want the whole world to have your phone
number, right? Remember, your university's digital platforms are often more public than
private so data protection rules apply. Data protection means: 'the laws that relate to
control over, access to, and use of data stored in computers'. And it's not just on your
university's platforms that you need to be secure. Just imagine if dishonest people got access
to your emails, bank account or credit card details! You could lose a lot of money like that.
Or if someone found out your personal details, they could pretend to be you and cause a
lot of loss or damage to you. And nobody likes to feel like a fool if they get tricked… I feel
properly silly for believing that fake lottery email – what an idiot!

The good news is there are lots of practical steps to take to be safe online. Think about all
your digital accounts – email, social media, banking, work, study. Now ask yourself, "How
strong is my password?" Be honest. Is it your name, your birthday, your pet's name? Hmm:
they could be quite weak. You might want to think about changing them to something
stronger. Mixing numbers, upper and lower-case characters, and special symbols is a good
idea. If you want to be really secure, use random numbers and letters. Now nobody would
give their cat a name like that! You could even use a short sentence, like this.

Personal details: only put your personal details into websites that you trust and that are
secure. Secure websites will begin with h-t-t-p-s. And some sites may provide a padlock in
the address bar. Always check the website address is spelt correctly: many fake websites change the address slightly, so you don't notice it's not the real website.

Be aware of scams and phishing. These are often emails from people you have never heard of or websites that ask you for personal or financial details. They may seem to offer something fantastic that you can claim for free. If something sounds too good to be true – then it probably is. And don't forget about the risks of ransomware. Ransomware means software the takes control of your computer and you have to pay criminals to get back control. And who would trust a criminal hacker to keep their word!

The good news is there are lots of tools to help keep you safe. Up to date anti-virus software is a must, and so is keeping your operating system updated. You can use password manager programs to generate strong passwords. But most importantly, use your own common sense: always remember that you need to stay safe digitally. Hey, look at that! I've won a brand new laptop worth thousands of pounds!! Wa- wait a minute!