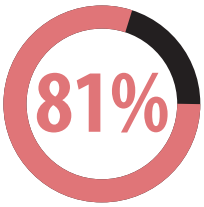
PAYMENT DATA SECURITY ESSENTIAL

Strong Passwords

WHAT'S THE RISK?



of hacking-related breaches leveraged either stolen and/or weak passwords

(2017 Verizon Data Breach Investigation Report)

The use of weak and default passwords is one of the leading causes of data breaches for businesses.

Passwords are essential for computer and payment data security. But to be effective, they must be strong and updated regularly.

Computer equipment and software out-of-the-box (including payment terminals) often come with vendor default or preset passwords such as "password" or "admin", which are commonly known and easily exploited by criminals.

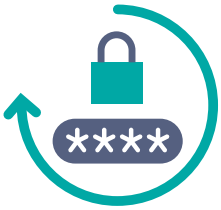
Typical default passwords that MUST BE changed:

[none]
[name of product/vendor]

1234 or 4321	pass
access	password
admin	root
anonymous	sa
database	secret
guest	sysadmin
manager	user

PASSWORD BEST PRACTICES

To minimize the risk of being breached, businesses should change vendor default passwords to strong ones, and never share them – each employee should have its own login ID and password.



Change your passwords regularly

Treat your passwords like a toothbrush. Don't let anyone else use them and get new ones every three months.

Don't share passwords

Insist on each employee having its own login ID and password – never share!

Make passwords hard to guess

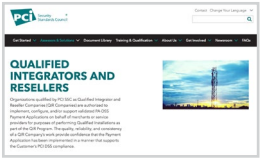
The most common passwords are "password", "password1" and "123456." Hackers try easily-guessed passwords because they're used by half of all people. A strong password has seven or more characters and a combination of upper and lower case letters, numbers, and symbols (like !@#$&*). A phrase that incorporates numbers and symbols can also be a strong password – the key is picking a phrase with specific meaning to you so it's easy to remember, like a favorite hobby, for example (like ILove2Fish4Trout!).

RESOURCES

Visit **pcissc.org/Merchants** for more resources

Vendors and service providers can help businesses identify default passwords and change them.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.



The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on strong passwords and other payment data security essentials.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by changing vendor default passwords to strong ones, and never sharing passwords.

PCI Security Standards Council