Passwords, Passwords, Passwords

FIDUCIARY™ TRUST

Information Security Insights

It seems everywhere you go online today you need to provide your email and create a password. In an effort to make sites more secure or to keep out spam and bots, many sites are asking you for this information. Not surprisingly, in an effort to remember a password, a lot of people use the same one, or a slightly different version of it, over and over again. The problem with reusing your password is your information is only as secure as the least secure place you use it.

Financial institutions utilize substantial security features, making them unappealing targets for cybercriminals. Instead, hackers focus on smaller groups that have fewer resources and, in many cases, a limited focus on security because most of the information you access on their site is not particularly valuable or revealing. For example, you may need to log in with your email and a password to access your children's soccer schedule, book a time at the local yoga studio, or see the calendar of events of a small organization to which you belong. Cybercriminals do not care about your kids' sports schedule or your yoga practices, so these sites may have lax security, thinking no one will bother to hack them. However, the hackers do want the email and password you use to access that information, so they can use it elsewhere.

Learn More:

For more information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

Rick Tyson
tyson@fiduciary-trust.com
617-292-6799

Password security is critical, and your email password may be the most important as it provides a view into many of your financial dealings

So how does a hacker get in and use your login credentials from your local site? First, many small websites are not up to date with the most recent security patches like larger firms are. The hacker exploits known vulnerabilities and breaks into the site. From there, they take your email address and password. Since they have your email, they know exactly where to go and will try to log in to your email account with the password you used on the local site. If it is the same or similar, they are in and can access all of your emails. From reading your mail, they can then find out where you bank and try the password there. Even if that does not work they can try resetting your passwords and have the new password sent to the same email account they are now accessing. Fortunately, banks have introduced some new security measures, like multi-factor authentication (such as texting you a one-time code to use when accessing your account), that make it harder for cybercriminals to reset your passwords just by getting into your email. However, criminals have other ways to engineer attacks.

We recently learned of someone, whom we'll call Bob, who almost fell victim to a hacker who was able to access his email account. The hacker read Bob's emails and noticed Bob was having renovations completed by a contractor. Bob would receive invoices in his email and send payment. The criminal established an email account that looked similar to the real business and then created a fake invoice that looked exactly like the real one, with one small difference – they changed the payment instructions. Bob received the bill and was about to pay it, but luckily ended up calling the firm about another issue and realized during the conversation that the invoice was fraudulent. This type of scam is effective because it avoids a much of a bank's security. The bank receives a valid instruction from the client and sends payment accordingly. In this instance, there is no way for the bank to know the client had been tricked into the request.

Password security is critical, and your email password may be the most important as it provides a view into many of your financial dealings. Here are a few steps you can take to protect yourself.

1. **Ensure your passwords are unique for each online account.** It is especially important that passwords for email accounts and financial institution accounts not only be distinct but also very different from each other, given the higher risks if a bad actor were to obtain access to these accounts.
2. **Do not ignore notices** that "someone has signed onto your account from a different device." Well-secured sites will warn you if they detect someone logging on to your account from a device that has never been used before. This could be someone trying to access your information. Take a look at it and determine if it was a legitimate log-in. If it was not, change your password immediately.
3. **Turn on multi-factor authentication if a site makes it available.** With multi-factor authentication, every time you or a bad actor logs in from a new location they will send you a code, usually a text to your phone number on file, to confirm that it's really you.
4. **Choose robust passwords.** Hackers have become more sophisticated and will try to guess your password based on typical behavior patterns. In the early days, they would try options such as password1234 and variations on that theme. But now, given decades of experience, they know what passwords people prefer to use. Months, seasons, and upcoming holidays are common. If your password

Learn More:

Access our full library of insights at fidtrustco.com/insights

Author

Robert Jeffers,
Chief Operating Officer

is something like MayMay2022! or Memorialday2022, you should consider changing it immediately. If criminals know where you are located, they will also try local sports teams. For example, in Boston, RedSox2022, Bruins#1, and Patroits1234 would all be poor choices. One effective approach can be to think of a word and then create a string of unrelated words. For example, let's say you have a cat named Tom – you might create a password like TreeOverMountain. Long passwords are generally more secure, provided they are not easy for someone to guess.

Given the importance of maintaining the security of your online accounts, it is clearly necessary to maintain strong passwords and regularly change them. In addition, keeping an eye out for suspicious communications is also paramount. While you cannot eliminate all risks, taking these steps can significantly reduce the likelihood of an undesirable outcome. At Fiduciary Trust, we take information security seriously and have numerous safeguards in place to protect client information and account access. ■

Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

Rick Tyson
tyson@fiduciary-trust.com
617-292-6799

FIDUCIARY™ TRUST