TECH TALK MONTHLY



How Hackers Keep Access to Your Email After You Change the Password

Inside:

- How to Make Sure Your Business Owns Its Domain Name
- What to Ask a Software Vendor After They Report a Data Breach
- Why Shared Logins Are a Security Risk for Your Business
- How to Protect Your Business Social Media Accounts From Hackers
- How to Move Offices Without Disrupting Your IT

What's Inside

Page 1:

- ***How Hackers Keep Access to Your Email After You Change the Password***

Page 2:

- ***How to Make Sure Your Business Owns Its Domain Name***

Page 3:

- ***What to Ask a Software Vendor After They Report a Data Breach***

Page 4:

- ***Why Shared Logins Are a Security Risk for Your Business***

Page 5:

- ***How to Protect Your Business Social Media Accounts From Hackers***

Page 6:

- ***How to Move Offices Without Disrupting Your IT***

Dear Business Owner 👋

Many business systems are set up by whoever needs them first. An employee may register the domain, while a marketing agency receives access to Facebook and Instagram. A login may be shared because that is how the account has always worked.

These arrangements can continue for years without causing an obvious problem. Then an employee leaves, a supplier reports a breach, or someone gets into an email account. The business needs to know who owns each account, who can still access it, and how to remove that access.

This month's newsletter will help you answer those questions. We explain why changing an email password may not sign an attacker out, how to confirm that your business controls its domain name, and what to ask after a software vendor reports a data breach. We also cover shared logins, social media account security, and the IT planning that should happen before an office move.

Start with the accounts that affect your email, website, payments, customer information, and public communications. Confirm who controls each one, make sure recovery details belong to the business, and remove access that is no longer needed.

If you would like help checking any of these areas, give us a call.

Stay safe,



Antonio Loffi-Lara

Antonio Loffi-Lara
CTO, Oasis Technologies, Inc.

DID YOU KNOW ?

The world's first website was hosted on Tim Berners-Lee's NeXT computer at CERN. It explained the World Wide Web project, and CERN restored it in 2013.

GET IN TOUCH

405.996.7124

oasis.tech/tony

tlara@oasis.tech

HOW HACKERS KEEP ACCESS TO YOUR EMAIL AFTER YOU CHANGE THE

PASSWORD

Changing the password is one of the first things to do when someone gets into a business email account. It stops the old password from being used for a new login, but it may not remove other access the attacker set up while they controlled the account.

They may still be signed in through a browser or email app. They could have created a forwarding rule, connected an outside application, added a recovery method, or given another account permission to use the mailbox.

Until those settings are checked, the attacker may still be able to read messages, receive copies of new email, or regain access later.

SIGN OUT ACTIVE SESSIONS

Email services use sessions so you do not have to enter your password whenever you open the inbox. Depending on the provider, a session may continue working until it expires or an administrator revokes it.

Ask your IT provider to revoke the account's active sessions and sign-in tokens through the email administration tools. If the employee's computer may contain malware, start the recovery from another device and have the affected computer checked before anyone signs in again.

CHECK MAILBOX RULES AND FORWARDING

An attacker can create a rule that forwards incoming email to another address. The rule may send every message, or it may only target words such as "invoice," "payment," or "password reset." Another rule could hide security alerts or customer replies in a folder the employee rarely opens.

Review forwarding addresses, inbox rules, filters, and automatic replies. Microsoft 365 administrators should also check for hidden inbox rules through the administration tools.

REVIEW CONNECTED APPS AND MAILBOX ACCESS

Scheduling tools, mobile apps, and customer systems can be given permission to use an email account. These connections often work through OAuth, so the application does not need the user's password.



Remove any connected application the business does not recognize or use. Check mailbox delegates and sending permissions too. Because a delegate signs in through their own account, changing the mailbox owner's password does not remove that access.

CHECK RECOVERY AND SIGN-IN METHODS

Ask the employee to confirm every phone number, recovery email address, authenticator app, passkey, security key, and registered device. Remove anything they cannot identify.

Then review sent, deleted, draft, junk, and archived messages, along with sign-in logs and security alerts. Look for password resets, unusual payment requests, and messages the employee did not send.

If false messages went to customers, suppliers, or employees, contact them through a trusted channel. Tell them which messages were fraudulent and whether they need to ignore a payment request, delete a file, or change a password.

Before the employee signs in again, require multifactor authentication. Use passkeys or physical security keys where the email service supports them.

HOW TO MAKE SURE YOUR BUSINESS OWNS ITS DOMAIN NAME

Customers use your domain name to reach your website and email your staff. The registration may go untouched for years while everything continues working.

Problems arise when the domain sits in an account controlled by an employee or supplier. If that relationship ends, your business may depend on them to renew, change, or transfer the domain.

Check it now, while the website and email are working normally.



FIND THE REGISTRAR

The registrar is the company that maintains the domain registration. For most generic domains, such as .com, .net, and .org, you can identify it through the ICANN Lookup tool. Country-code domains may use their local registry's lookup service.

Your registrar may be different from your website host, DNS provider, and email provider. Record which company handles each service.

CONFIRM THE BUSINESS CONTROLS THE ACCOUNT

Someone inside your business should be able to sign in to the registrar account and see the domain. Check that the company can update its contact details, payment method, renewal settings, and nameservers.

Access to WordPress or a website hosting account does not necessarily include control of the domain registration. Sign in to the registrar account itself.

The recovery details should belong to the business. Store the password and recovery codes in the company password manager, and require multifactor authentication.

CHECK THE REGISTRATION AND RENEWAL DETAILS

A domain registration gives the registrant the right to use the name for a set period. Confirm that the registered organization and contact information are correct.

Check the expiry date, auto-renewal setting, and payment method. Renewal reminders should reach a monitored address. Automatic renewal will fail if the saved card has expired.

REVIEW DNS ACCESS

DNS settings direct visitors to your website and tell email services where to deliver messages. A change to those records can interrupt both services, so DNS access needs to remain under company control.

Record where the DNS is managed and who can change it. Ask your IT provider before editing any records.

IF A SUPPLIER CONTROLS THE DOMAIN

Ask the supplier to move the domain into a registrar account controlled by the business. Plan the transfer with your IT provider, who can monitor the website and email during the change.

Keep contracts, invoices, payment records, and registration emails that connect the domain to your company. The registrar may request this evidence, and an ownership dispute may require legal advice.

Review the account every year and whenever access changes. Recheck the expiry date, payment method, and recovery options.

WHAT TO ASK A SOFTWARE VENDOR AFTER THEY REPORT A DATA BREACH

A breach notice from your payroll provider, accounting platform, CRM, or another software vendor may arrive before the company has finished its investigation. You still need enough information to decide what your business should do next.

First, confirm that the notice is genuine. Go to the vendor's website or customer portal using an address you already know. Criminals sometimes send fake password-reset or support messages after a public breach announcement.

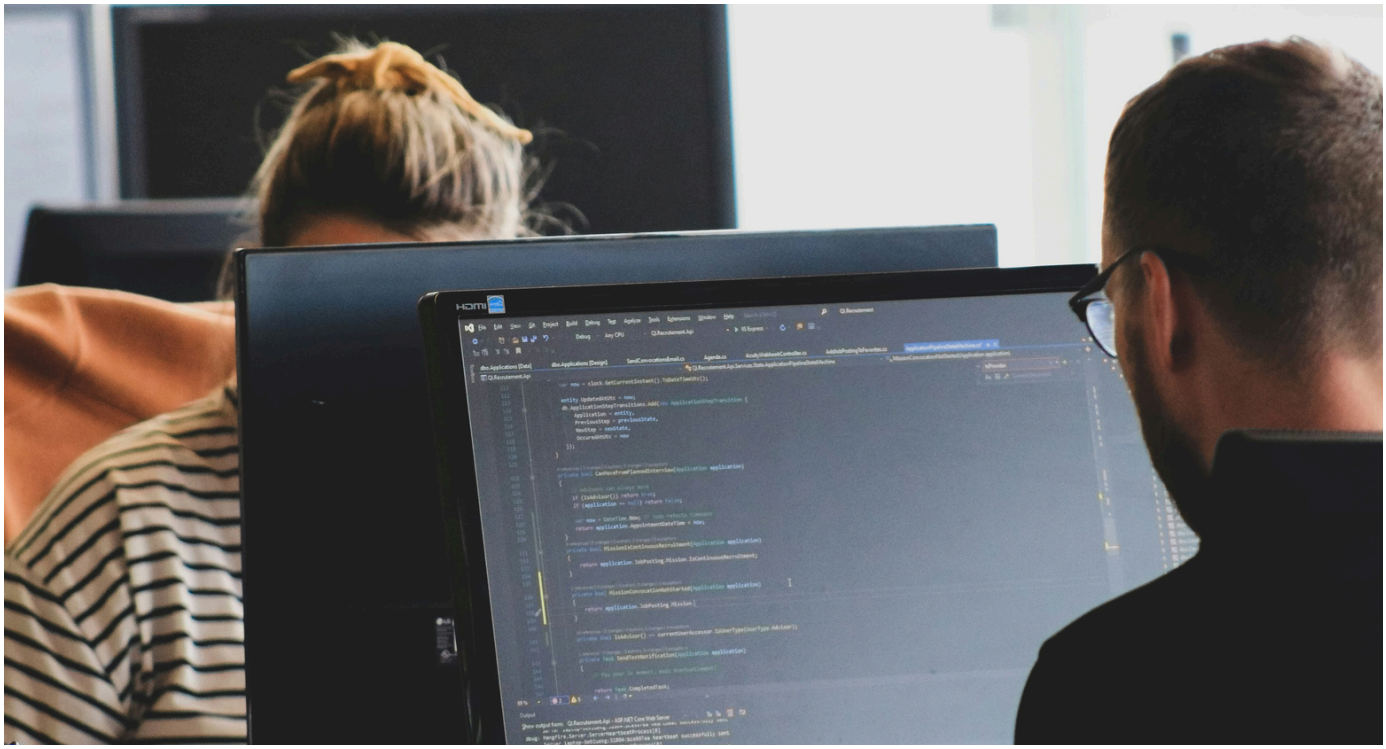
Once the notice is confirmed, ask whether your business was affected and what information was involved. Find out when the unauthorized access began, when the vendor detected it, and when the vendor contained it. Ask whether the person could view, copy, change, or delete information.

Also ask whether API keys, access tokens, single sign-on connections, or integrations with your email, accounting, payment, storage, or backup systems need to be reset or revoked.

If the vendor says there is no evidence that information was copied or misused, ask what logs support that statement and whether they cover the full period under investigation.

Get the vendor's instructions in writing. You may need to install an update, reset certain accounts, review transactions, disconnect an integration, or warn employees about related scams.

Keep the original notice, later updates, your questions, the vendor's answers, and a record of what your business did. Depending on the information involved and where your business operates, you may also need advice from your IT provider, insurer, privacy specialist, or legal adviser.



WHY SHARED LOGINS ARE A SECURITY RISK FOR YOUR BUSINESS

A shared login may seem convenient when several employees need the same software, mailbox, or website account. If a payment changes, customer information is downloaded, or the account signs in from an unfamiliar device, the account history may show every action under the same username.

Shared passwords also spread through messages, documents, browsers, and personal password stores. When an employee leaves, the password must be changed everywhere it is used or that person may keep access.

Give each employee their own account wherever the software allows it. Individual accounts let you remove one person's access, apply multifactor authentication properly, match permissions to the employee's work, and trace activity to a named user.

If an older system only provides one login, keep the password in a business password manager. Limit access to the employees who need it, name an owner for the account, and change the password whenever someone leaves the authorized group.



HOW TO PROTECT YOUR BUSINESS SOCIAL MEDIA ACCOUNTS FROM HACKERS

Business social media accounts often pass through several employees and agencies. Years later, the recovery email may belong to someone who has left, while former suppliers still have permission to post or run advertising.

List every company page, profile, channel, and advertising account. Record who owns it, who has administrator access, which business email and phone number are used for recovery, and which outside applications can publish content.

Give each person their own access instead of sharing a password. Use the lowest role that allows them to do their work, require multifactor authentication and remove access as soon as an employee or agency leaves.

Require multifactor authentication on the recovery email account too. If someone gets into that inbox, they may be able to reset the social media password and take control of the account.

Review access and connected apps regularly. Keep the platform's official recovery instructions and your advertising account details somewhere your team can find them if an account is compromised.



HOW TO MOVE OFFICES WITHOUT DISRUPTING YOUR IT

Moving the computers is only one part of an office move. Your staff will also need working internet, Wi-Fi, phones, printers, cloud applications, payment systems, and any network-connected security or building equipment.

Involve your IT provider before the move date is fixed. Ask them to inspect the new office, check the cabling and power, plan Wi-Fi coverage, and confirm where the network equipment will go.

Order the internet connection early. Installation may require a site survey, building approval, cabling work, and an engineer visit. Keep the old connection active until the new service has been installed and tested.

Make a list of the systems the business needs each day, including phones, card terminals, alarms, door access, cameras, meeting-room equipment, and specialist software. Confirm what each one needs at the new address.

Back up important data before any equipment is disconnected, and check that the latest backups can be restored. Label



computers, monitors, cables, phones, power supplies, and adapters so the correct parts arrive together.

Test the new office before employees arrive. Sign in to key applications, make calls, join a video meeting, print and scan, and check payment or booking systems. Arrange support for the first working day, when staff may need help connecting to the network or finding shared equipment.

Thank You!

Thanks for taking the time to read this month's newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW

OASIS TECHNOLOGIES

405.948.6500

info@oasis.tech

oasis.tech

6317 NW 23rd St.
Bethany, OK 73008