Guia de Segurança da Informação para

PROFESSORES

SEGURANÇA DIGITAL
EDUCAÇÃO DO PARANÁ

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Ilustração

Will Stopinski
Leandro Alves de Almeida
Debora Bacchi Camillo

Projeto Gráfico/Diagramação

Joise Nascimento
Silvio Turra

Conteúdo e Elaboração

GOVERNADOR DO ESTADO DO PARANÁ

Carlos Massa Ratinho Junior

Secretário de Estado da Educação

Professor Roni Miranda Vieira

Diretor-Geral

João Luis Giona Junior

Diretor de Educação

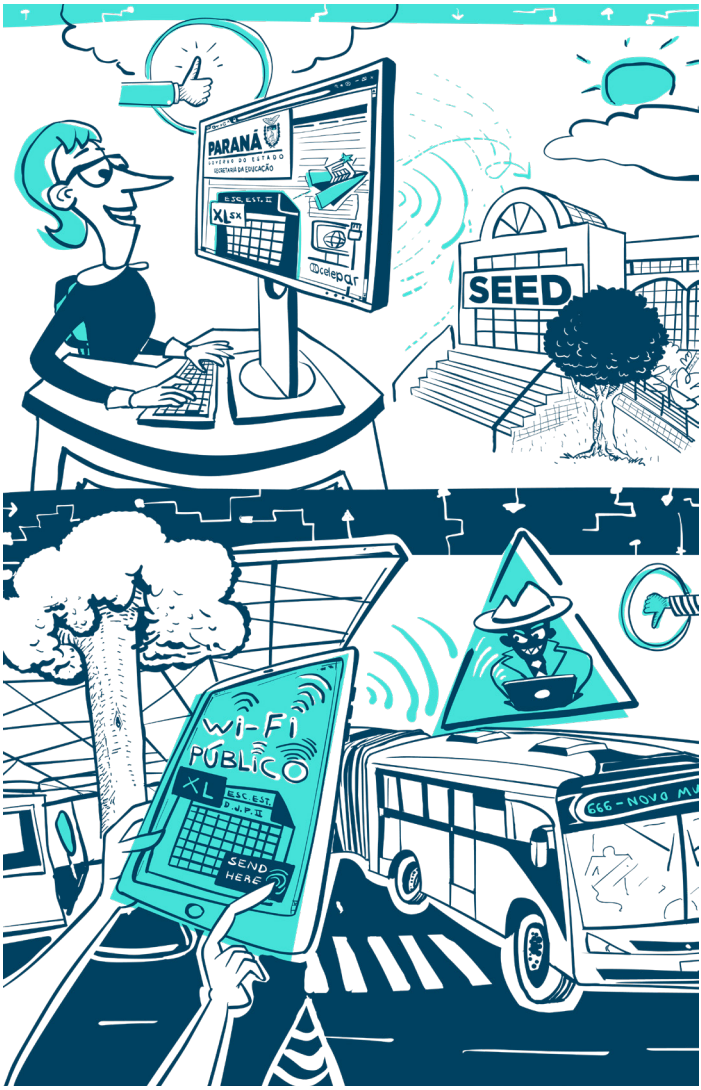
Anderfábio Oliveira dos Santos

Diretor de Tecnologia e Inovação

Claudio Aparecido de Oliveira

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Guia prático de segurança da informação desenvolvido para professores da rede pública. Aborda proteção de contas, segurança de dados, defesa contra malware, uso responsável de redes sociais e gerenciamento de dispositivos, com medidas simples para proteger informações digitais de professores e alunos.



Sumário

Este guia apresenta medidas de segurança práticas para o cotidiano profissional dos professores. Os capítulos abordam necessidades específicas dos educadores em ambiente digital, considerando a realidade das escolas públicas brasileiras.

Introdução à Segurança da Informação

A segurança da informação tornou-se uma preocupação fundamental no ambiente educacional moderno. Com a digitalização crescente dos processos pedagógicos e administrativos, professores lidam diariamente com dados sensíveis de alunos, materiais didáticos originais e informações institucionais confidenciais.

Proteger esse patrimônio digital não é apenas uma questão técnica, mas também ética e legal. Este guia foi desenvolvido para oferecer orientações práticas que possam ser implementadas no dia a dia, mesmo por aqueles com conhecimentos básicos de tecnologia. Nosso objetivo é fortalecer a cultura de segurança digital nas escolas públicas brasileiras.

Por que a Segurança Digital é Importante para Professores

Proteção de Dados Sensíveis

Professores lidam com informações confidenciais dos alunos, incluindo notas, frequência e, em alguns casos, informações familiares e de saúde.

Preservação de Material Didático

Anos de planejamentos, atividades e avaliações representam um valioso patrimônio intelectual que merece proteção adequada.

Modelo para os Alunos

Ao demonstrar boas práticas de segurança digital, os educadores ajudam a formar uma geração mais consciente sobre os riscos cibernéticos.

Prevenção de Incidentes

Adotar medidas preventivas reduz significativamente o risco de vazamentos de dados, perda de informações e outras situações que podem comprometer o trabalho pedagógico.

Proteção de Contas e Senhas: Fundamentos

A primeira linha de defesa para sua segurança digital está nas senhas que você utiliza. Como educador, você acessa diariamente sistemas de gestão escolar, e-mails institucionais, e plataformas educacionais que contêm dados sensíveis de alunos. Pesquisas mostram que 65% dos professores reutilizam senhas entre contas pessoais e profissionais, e 40% usam informações óbvias como datas de nascimento ou nomes de familiares, práticas que comprometem gravemente a segurança dos dados pedagógicos.

Nesta seção, você aprenderá técnicas específicas para criar senhas robustas usando combinações de 12 caracteres com letras, números e símbolos. Mostraremos como configurar a verificação em duas etapas no e-mail institucional e no sistema de gestão escolar de sua rede, além de apresentar gerenciadores de senha gratuitos compatíveis com a infraestrutura típica de escolas públicas. Estas ferramentas protegerão não apenas suas provas e materiais didáticos, mas também informações confidenciais como histórico escolar e registros de atendimento especializado de seus alunos.

Criando Senhas Fortes e Exclusivas

O que faz uma senha forte?

- Mínimo de 12 caracteres
- Letras maiúsculas e minúsculas
- Números e símbolos especiais
- Evitar sequências e dados pessoais

Estratégias para senhas memoráveis

- Frases completas (ex: “MeuFilhoNasceuEm2015!”)
- Substitua letras por números/símbolos similares
- Combine palavras não relacionadas com números
- Crie um sistema para diferenciar senhas por serviço

Importante: use senhas únicas para cada conta. Uma senha comprometida em um serviço não deve afetar os demais.

Verificação em Duas Etapas: Uma Camada Extra de Proteção

A verificação em duas etapas (ou autenticação de dois fatores - 2FA) adiciona uma camada extra de segurança às suas contas, exigindo além da senha, um segundo elemento para confirmar sua identidade. Assim, mesmo que alguém descubra sua senha, não conseguirá acessar sua conta sem esse segundo fator.

Para contas da Secretaria da Educação, esta verificação geralmente envolve um código enviado por aplicativo, mensagem SMS ou e-mail. Ative esta proteção em todas as plataformas profissionais, especialmente e-mail, drives e sistemas escolares, reduzindo o risco de acesso não autorizado.

Como Ativar a Verificação em Duas Etapas

Acesse as configurações de segurança

Procure nas configurações ou preferências da conta as opções de segurança ou privacidade.

Selecione a opção de verificação

Geralmente chamada “verificação em duas etapas”, “autenticação de dois fatores” ou “login em duas etapas”.

Escolha o método de verificação

Pode ser por SMS, aplicativo autenticador (como Google Authenticator) ou chave física.

Siga as instruções de configuração

Geralmente envolve verificar um código recebido para confirmar que o processo funciona.

Salve os códigos de recuperação

Guarde-os em local seguro para usar caso perca acesso ao seu dispositivo de verificação.

Gerenciadores de Senhas: Organizando sua Vida Digital

Gerenciadores de senhas armazenam suas senhas de forma segura, exigindo apenas uma senha mestra para acessá-las. Eles geram senhas fortes, eliminam a necessidade de memorizar múltiplas senhas e sincronizam suas credenciais entre vários dispositivos.

Existem opções gratuitas como 1Password, Bitwarden, LastPass, que podem ser integradas em navegadores. Para professores, recomendamos serviços com criptografia de ponta a ponta que permitam organizar senhas por categorias (pessoais, trabalho, financeiras), facilitando a gestão da sua vida digital.

Erros Comuns na Gestão de Senhas

Salvar senhas no navegador

Embora conveniente, esta prática pode ser arriscada, especialmente em computadores compartilhados. Qualquer pessoa com acesso físico ao dispositivo poderá acessar suas contas se não houver proteção adicional.

Anotar senhas em papel ou arquivos desprotegidos

Manter uma lista de senhas em um arquivo de texto comum ou em anotações físicas expostas representa um risco significativo, pois qualquer pessoa que tenha acesso ao seu espaço pode visualizá-las.

Compartilhar senhas por mensagem ou e-mail

Estes canais não são seguros para transmitir informações sensíveis. Mensagens podem ser interceptadas ou permanecer nos servidores por tempo indeterminado.

Códigos de Backup: Sua Rede de Segurança

Quando você ativa a verificação em duas etapas, recebe códigos de backup essenciais para recuperar o acesso caso perca seu dispositivo de verificação ou o número de telefone cadastrado.

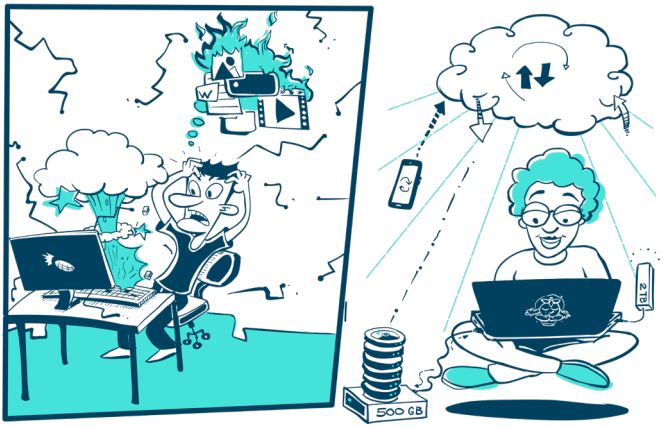
Imprima estes códigos e guarde-os em local fisicamente seguro, como um cofre ou gaveta com chave. Evite mantê-los apenas em formato digital para não criar dependência do mesmo dispositivo que está tentando recuperar. Para contas institucionais importantes, considere informar um contato de confiança da TI escolar sobre a localização desses códigos para emergências. (Validar).

Segurança de Dados: Protegendo Informações Pedagógicas

Como professor, você gerencia diversos dados pedagógicos valiosos: planos de aula, atividades, avaliações e registros de alunos. Esses materiais representam seu patrimônio intelectual e profissional, merecendo proteção adequada.

Apresentaremos estratégias para proteger seus dados contra perdas acidentais, falhas de hardware, ataques cibernéticos e acessos não autorizados. Essas práticas garantirão que seu trabalho permaneça seguro e acessível, evitando a frustração de ter que recriar materiais perdidos.

A Importância dos Backups Automáticos



Benefícios dos backups automáticos

- Elimina a necessidade de cópias manuais
- Garante regularidade nas cópias
- Minimiza risco de perda de dados
- Permite recuperar versões anteriores

Opções para professores

- Google Drive (e-mail institucional)
- Microsoft OneDrive (pacote Office 365 Educacional)
- Sistemas da Secretaria da Educação
- Discos externos com backup agendado

Configure documentos importantes para sincronizar com a nuvem, garantindo que alterações sejam salvas local e remotamente.

Configurando Backups Automáticos

Identifique seus arquivos essenciais

Priorize documentos pedagógicos, registros de alunos, planos de aula e materiais didáticos desenvolvidos por você.

Escolha um serviço de armazenamento

Prefira serviços aprovados pela sua instituição, como Google Drive ou Microsoft OneDrive vinculados ao e-mail institucional.

Instale aplicativos de sincronização

Tanto Google quanto Microsoft oferecem aplicativos que criam pastas sincronizadas automaticamente no seu computador.

Organize seus arquivos nas pastas sincronizadas

Mova seus documentos importantes para estas pastas ou configure o salvamento automático nestes locais.

Verifique regularmente se a sincronização está funcionando

Confira ocasionalmente se os arquivos estão sendo atualizados na nuvem, especialmente após alterações importantes.

Protegendo Pastas e Arquivos com Senhas

Para proteger arquivos sensíveis, como avaliações ou dados confidenciais de alunos, utilize criptografia ou senhas. No Microsoft Office, acesse "Arquivo > Informações > Proteger Documento > Criptografar com Senha". Para PDFs, use a opção de segurança durante a criação.

Para múltiplos arquivos, crie arquivos ZIP com senha usando programas gratuitos como 7-Zip. Use senhas fortes e diferentes das suas contas principais. Para documentos extremamente sensíveis, considere softwares de criptografia como VeraCrypt, que criam "cofres" virtuais no computador.

Compartilhamento Seguro de Materiais

Utilize plataformas institucionais

Priorize ambientes virtuais de aprendizagem ou plataformas aprovadas pela Secretaria da Educação para compartilhar materiais didáticos com os alunos.

Configure permissões de acesso

Ao compartilhar documentos na nuvem, defina permissões adequadas: “apenas visualização” para materiais que não devem ser alterados e “edição” apenas quando necessário.

Use links expiráveis

Quando possível, configure links de compartilhamento para expirarem após determinado período, garantindo que o acesso seja temporário.

Verifique destinatários

Ao enviar materiais por e-mail, confirme sempre se os endereços dos destinatários estão corretos para evitar compartilhamento indevido.

Gerenciando Informações Sensíveis de Alunos

Sistemas Oficiais

Sempre utilize os sistemas oficiais da Secretaria da Educação para registrar e armazenar dados sensíveis, como informações pessoais, histórico médico e avaliações dos alunos.

Exclusão Segura

Exclua de forma segura os dados sensíveis quando não forem mais necessários, utilizando métodos que impossibilitem a recuperação das informações.

Proteção com Senha

Quando for inevitável trabalhar com informações sensíveis localmente, utilize arquivos protegidos por senha e mantenha-os apenas pelo tempo necessário.

Anonimização

Considere a pseudonimização ou anonimização dos dados sempre que possível, substituindo nomes completos por iniciais ou códigos em documentos temporários.

Organizando Seus Arquivos Digitais

A boa organização facilita a localização, backup e recuperação de materiais em caso de incidentes.

Estrutura de pastas recomendada

Organize seus arquivos em hierarquia: **Ano Letivo > Turma > Disciplina > Tipo de Material**. Separe avaliações, planos de aula e atividades em pastas distintas.

Áreas de trabalho específicas

Crie uma área dedicada para materiais em desenvolvimento e uma seção separada para arquivos compartilhados com outros professores ou alunos.

Práticas de nomenclatura

Use datas no formato **AAAA-MM-DD (ano-mês-dia)**, inclua identificadores de turma/disciplina e números de versão (v1, v2). Evite caracteres especiais (/, \, :, *, ?) nos nomes dos arquivos.

Proteção contra Códigos Maliciosos: Ameaças Digitais

Códigos maliciosos, também conhecidos como malware, representam uma ameaça constante para seus dados e privacidade digital. Estes incluem vírus, ransomware (que sequestra seus arquivos exigindo pagamento), spyware (que espiona suas atividades) e outros programas prejudiciais que podem comprometer seu trabalho pedagógico e informações sensíveis.

Professores são alvos particularmente valiosos para ataques cibernéticos devido ao acesso que possuem a sistemas educacionais e dados de estudantes. Esta seção apresenta medidas essenciais para proteger seus dispositivos contra estas ameaças, garantindo a continuidade de suas atividades profissionais e a segurança das informações sob sua responsabilidade.

A Importância dos Antivírus

Proteção em tempo real

Antivírus modernos monitoram constantemente seu sistema para identificar comportamentos suspeitos e bloquearam ameaças antes que causem danos.

Verificações programadas

Além da proteção contínua,configure verificações completas periódicas para identificar malwares que possam estar ocultos em seu sistema.

Proteção de navegação

Muitos antivírus incluem extensões para navegadores que alertam sobre sites potencialmente perigosos antes que você os acesse.

Atualizações automáticas

Certifique-se de que seu antivírus estáconfigurado para atualizar automaticamente tanto o programa quanto sua base de definições de vírus.

Opções de Antivírus para Educadores

Windows Defender

Incluso nas versões do Windows 10 e 11, oferece proteção adequada para a maioria dos educadores

Avast Free Antivirus

Solução gratuita com recursos de proteção em tempo real para educadores

AVG Antivirus Free

Opção gratuita com proteção contra malware para dispositivos educacionais

Avira Free Security

Ferramenta de segurança gratuita com funcionalidades para proteção de dados

Usuários Mac contam com o XProtect integrado ao sistema, mas podem complementá-lo com Malwarebytes. Educadores devem verificar licenças institucionais disponíveis na sua Secretaria de Educação ou consultar o departamento de TI para recomendações específicas para o ambiente escolar.

Mantendo Sistemas e Aplicativos Atualizados

Atualizações de software não apenas adicionam recursos, mas principalmente corrigem vulnerabilidades de segurança. Quando fabricantes descobrem falhas, desenvolvem correções distribuídas via atualizações. Ignorá-las expõe seu sistema a ataques conhecidos.

Configure seu sistema operacional para instalar atualizações automaticamente fora do horário de aulas. Mantenha seus aplicativos atualizados, especialmente navegadores, editores de texto e programas de e-mail, que são frequentemente alvos de phishing. Ative as atualizações automáticas nas configurações destes programas sempre que possível.

Como Identificar Links e Mensagens Suspeitas

Verifique o remetente

Desconfie de e-mails de remetentes desconhecidos ou com endereços levemente diferentes dos oficiais (como secretaria-educacao.com em vez de secretariadaeducacao.gov.br).

Analise o conteúdo

Erros gramaticais, formatação estranha ou tom urgente (“aja imediatamente”) são sinais de alerta. Comunicações oficiais geralmente são formais e sem pressão indevida.

Inspecione links antes de clicar

Passe o mouse sobre um link (sem clicar) para ver o endereço real. Se for diferente do texto exibido ou parecer estranho, não clique.

Tenha cuidado com anexos

Não abra anexos inesperados, especialmente se tiverem extensões executáveis **(.bat, .exe, .js, .msi).** Verifique com o remetente por outro canal (telefone) se ele realmente enviou o arquivo.

Configurando Seu Navegador para Maior Segurança

Mantenha o navegador atualizado

Verifique regularmente se seu Chrome, Firefox, Edge ou Safari está na versão mais recente. A maioria atualiza automaticamente, mas é bom confirmar.

Ative a proteção contra phishing e malware

Nas configurações de segurança do navegador, certifique-se de que as opções de proteção contra sites perigosos estejam ativadas.

Use extensões de segurança

Considere adicionar uBlock Origin para bloquear anúncios potencialmente maliciosos ou HTTPS Everywhere para conexões mais seguras.

Configure permissões de sites

Restrinja o acesso de sites à sua câmera, microfone e localização, permitindo apenas quando necessário e para sites confiáveis.

Desative o preenchimento automático de dados sensíveis

Nas configurações de formulários e senhas, desative o preenchimento automático para informações financeiras e outras dados sensíveis.

O Perigo do Ransomware para Educadores

Ransomware é um malware que criptografa arquivos e exige pagamento para restaurar o acesso. Para professores, isso pode resultar na perda de materiais didáticos, avaliações e registros de alunos.

Como o pagamento não garante a recuperação e não é recomendado, a prevenção é essencial. Além das medidas de segurança já mencionadas, implemente a regra 3-2-1 de backup: três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia armazenada em local separado ou na nuvem.

Uso Seguro de Redes Sociais: Navegando o Ambiente Digital

Redes sociais são ferramentas valiosas para educadores compartilharem experiências, criarem comunidades de aprendizagem e se comunicarem com alunos e responsáveis, mas apresentam riscos à privacidade e segurança das informações.

Conheça estratégias para usar redes sociais de forma produtiva e segura, protegendo sua privacidade pessoal, a imagem da instituição e os dados dos estudantes, encontrando equilíbrio entre os benefícios digitais e uma presença online responsável.

Educação Digital para Alunos

Incorpore segurança digital ao currículo

Reserve momentos para discutir com os alunos sobre privacidade online, comportamento responsável nas redes e como proteger informações pessoais. Adapte as discussões de acordo com a faixa etária.

Discuta cyberbullying e suas consequências

Aborde o tema do assédio online, incentivando o respeito nas interações digitais e orientando sobre como agir ao presenciar ou sofrer situações de cyberbullying.

Seja modelo de comportamento digital

Demonstre boas práticas em sua própria utilização de tecnologia, mostrando como navegar com segurança e respeitar a privacidade alheia no ambiente digital.

Ensine verificação de informações

Desenvolva o pensamento crítico dos alunos para identificar notícias falsas, verificar fontes e compreender que nem tudo na internet é confiável.

Configurações de Privacidade nas Redes Sociais

Facebook

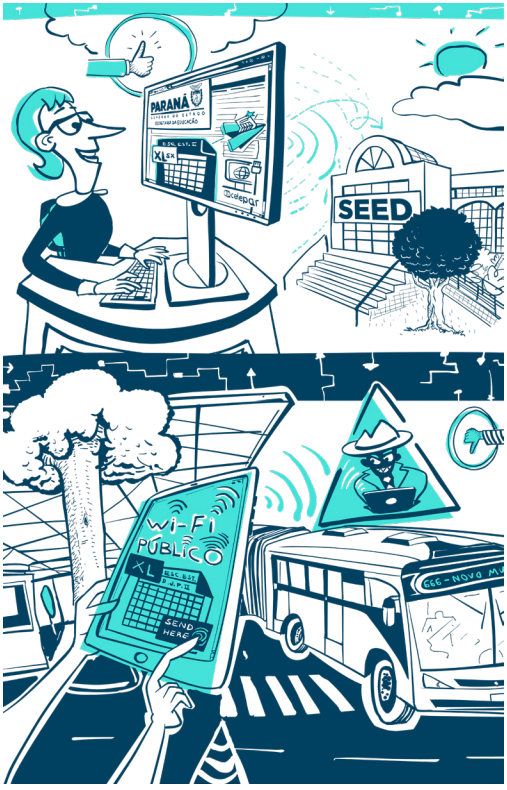
- Acesse "Configurações e privacidade"
- Restrinja visualização de publicações
- Limite solicitações de amizade
- Desative buscas externas do seu perfil

Instagram

- Considere uma conta privada
- Controle marcações em publicações
- Gerencie solicitações de mensagens
- Revise seguidores periodicamente

Verifique estas configurações com frequência devido a atualizações das plataformas. Mantenha contas profissionais separadas das pessoais.

Diretrizes para Compartilhamento de Conteúdo Escolar



Ao compartilhar atividades escolares, tenha extremo cuidado com imagens e informações dos alunos. Obtenha autorização formal dos responsáveis antes de publicar fotos ou vídeos com estudantes, mesmo em grupos fechados. Priorize mostrar os trabalhos sem expor rostos, focando nas produções.

Evite nomes completos ou informações identificáveis. Ao destacar projetos, use termos genéricos como “alunos do 5º ano” em vez de identificações específicas. Lembre-se que, mesmo com configurações de privacidade, o conteúdo digital pode ser compartilhado além do seu controle inicial.

Utilizando Grupos Fechados com Segurança

Verifique membros regularmente

Revise periodicamente a lista de participantes para garantir que apenas pessoas autorizadas (alunos, responsáveis ou outros educadores) estejam presentes.

Estabeleça regras claras

Defina e comunique diretrizes sobre o tipo de conteúdo permitido, comportamento esperado e finalidade do grupo.

Monitore as interações

Acompanhe as discussões e intervenha quando necessário para manter o ambiente seguro e produtivo para todos os participantes.

Limite informações sensíveis

Evite compartilhar no grupo dados que possam comprometer a segurança da instituição ou dos alunos, como horários específicos de atividades externas.

Separando Vida Pessoal e Profissional nas Redes

Manter perfis separados para uso pessoal e profissional é uma estratégia recomendada para educadores. Esta separação permite que você compartilhe conteúdo pessoal com amigos e familiares sem expor essas informações à comunidade escolar, enquanto mantém um perfil profissional adequado para interações com alunos, responsáveis e colegas de trabalho.

No perfil profissional, compartilhe apenas conteúdo relacionado à educação, conquistas profissionais e informações relevantes para a comunidade escolar. Evite expressar opiniões políticas polarizadoras, compartilhar detalhes da vida privada ou publicar conteúdo que possa ser mal interpretado. Lembre-se que, como educador, você representa não apenas a si mesmo, mas também sua instituição.

Riscos do Oversharing para Professores

Exposição excessiva de informações pessoais

Compartilhar detalhes como endereço, rotina diária ou informações familiares pode comprometer sua segurança física e digital, tornando-o vulnerável a pessoas mal-intencionadas.

Comprometimento da autoridade em sala de aula

Certas publicações podem afetar sua imagem profissional e a relação de respeito com alunos e responsáveis, especialmente conteúdo controverso ou inapropriado.

Vulnerabilidade a engenharia social

Informações compartilhadas podem ser usadas para criar ataques personalizados, como e-mails convincentes que parecem vir de pessoas conhecidas.

Permanência do conteúdo digital

Mesmo após excluir uma publicação, ela pode ter sido salva, compartilhada ou arquivada, permanecendo acessível indefinidamente.

Gerenciamento de Dispositivos: Proteção Física e Digital

Os dispositivos utilizados por educadores, sejam institucionais ou pessoais, frequentemente contêm informações sensíveis sobre alunos, materiais didáticos e dados administrativos da escola. Proteger adequadamente esses equipamentos é fundamental para garantir a segurança das informações educacionais.

Esta seção aborda estratégias para o gerenciamento seguro de dispositivos, incluindo práticas de proteção física, configurações de segurança recomendadas e procedimentos para situações de perda ou roubo. Implementar estas medidas reduz significativamente o risco de comprometimento de dados educacionais sensíveis e protege tanto sua privacidade quanto a dos seus alunos.

Dispositivos Institucionais vs. Pessoais

Vantagens dos dispositivos institucionais

- Geralmente possuem políticas de segurança pré-configuradas
- Suporte técnico disponível através da instituição
- Responsabilidade compartilhada em caso de incidentes
- Separação natural entre dados pessoais e profissionais

Cuidados com dispositivos pessoais

- Implemente as mesmas medidas de segurança dos institucionais
- Crie perfis ou contas separados para uso pessoal e profissional
- Considere usar aplicativos em "contêineres" para dados escolares
- Tenha cuidado especial ao conectar-se a redes públicas

Sempre que possível, utilize dispositivos institucionais para acessar sistemas da Secretaria da Educação, especialmente aqueles que contêm dados sensíveis de alunos ou informações administrativas confidenciais.

Configurando o Bloqueio de Tela

O bloqueio de tela é sua primeira linha de defesa contra acessos não autorizados em caso de dispositivos perdidos, roubados ou simplesmente deixados sem supervisão momentaneamente. Configure seus dispositivos para bloquearem automaticamente após um curto período de inatividade (recomendamos entre 2 a 5 minutos) e proteja o desbloqueio com um método seguro.

Em computadores, utilize senhas fortes ou PIN de no mínimo 6 dígitos. Em dispositivos móveis, aproveite recursos biométricos como impressão digital ou reconhecimento facial, mas sempre mantenha um PIN ou senha como método alternativo. Evite padrões de desbloqueio simples ou visíveis, como desenhos ou ligar pontos, que podem ser facilmente copiados por terceiros. Lembre-se de bloquear manualmente o dispositivo sempre que se afastar, mesmo que temporariamente ou por poucos minutos.

Localizando Dispositivos Perdidos ou Roubados

Android

Utilize o serviço “Encontre Meu Dispositivo” da Google. Acesse findmydevice.google.com com sua conta Google para localizar, bloquear ou apagar remotamente seu dispositivo Android.

Windows

Use o recurso “Encontre Meu Dispositivo” nas configurações de Contas. Certifique-se de que está ativado antes de qualquer incidente.

iOS (iPhone/iPad)

Ative o “Buscar iPhone” nas configurações iCloud. Em caso de perda, acesse icloud.com/find ou use o aplicativo “Buscar” em outro dispositivo Apple para localizar, bloquear ou apagar o dispositivo.

macOS

Configure o “Buscar Mac” nas preferências iCloud. Use o mesmo sistema do iOS para localizar ou apagar remotamente.

Ative esses recursos **antes** de qualquer incidente. Eles não podem ser habilitados remotamente após a perda do dispositivo.

Utilizando Tokens e Aplicativos de Autenticação

Tokens físicos e aplicativos de autenticação representam métodos avançados para proteger o acesso às suas contas mais importantes. Tokens físicos são pequenos dispositivos, geralmente conectados via USB ou Bluetooth, que verificam sua identidade durante o login. Já os aplicativos de autenticação, como Google Authenticator, Microsoft Authenticator ou Authy, geram códigos temporários no seu smartphone.

Para sistemas educacionais que contêm dados sensíveis de alunos, recomendamos a utilização desses métodos. Configure-os seguindo as instruções da plataforma e mantenha sempre um método alternativo de recuperação (como códigos de backup) em caso de perda do token ou do smartphone. Alguns sistemas educacionais já oferecem compatibilidade nativa com esses métodos de autenticação.

Cuidados com Dispositivos em Ambientes Escolares

Nunca deixe dispositivos desbloqueados

Mesmo em sala dos professores ou outros espaços considerados seguros, mantenha o hábito de bloquear manualmente seus dispositivos ao se afastar.

Tenha cuidado com observadores

Ao acessar informações sensíveis, como notas ou relatórios de alunos, posicione a tela de forma que outras pessoas não possam visualizar o conteúdo.

Evite conectar dispositivos desconhecidos

Pen drives e outros dispositivos externos podem conter malware. Utilize apenas equipamentos confiáveis ou verifique-os com antivírus antes de abrir arquivos.

Cuidado com redes Wi-Fi públicas

Evite acessar sistemas com dados sensíveis quando conectado a redes abertas. Use VPN ou conexão móvel própria para maior segurança.

Guarde dispositivos em locais seguros

Ao final do expediente, não deixe equipamentos à vista. Utilize armários com chave ou leve-os consigo quando possível.

Plano de Ação em Caso de Incidentes

Mesmo com todas as precauções, incidentes de segurança podem ocorrer. Ter um plano de ação predefinido ajuda a minimizar danos e a responder rapidamente. Se suspeitar que suas contas foram comprometidas, altere imediatamente suas senhas a partir de um dispositivo seguro e verifique atividades recentes em busca de ações não autorizadas.

Em caso de perda ou roubo de dispositivos, utilize as ferramentas de localização mencionadas anteriormente e notifique imediatamente o departamento de TI da sua instituição. Se dados sensíveis de alunos foram potencialmente expostos, informe a coordenação escolar para que medidas apropriadas sejam tomadas. Documente o incidente, incluindo datas, horários e ações realizadas, para referência futura e possíveis procedimentos administrativos.

Conclusão: Desenvolvendo uma Cultura de Segurança Digital

A segurança da informação não é apenas um conjunto de regras e ferramentas, mas uma mentalidade que deve ser cultivada continuamente. Como educador, você tem a oportunidade de não apenas proteger seus próprios dados e os de seus alunos, mas também de inspirar uma nova geração a adotar práticas digitais seguras e responsáveis.

Compartilhe seu conhecimento com colegas, participe de capacitações quando disponíveis e mantenha-se atualizado sobre novas ameaças e soluções. A colaboração entre educadores fortalece o ambiente digital escolar como um todo. Lembre-se que pequenas ações consistentes — como usar senhas fortes, verificar links antes de clicar e manter sistemas atualizados — fazem uma grande diferença na prevenção de incidentes. A segurança digital é uma jornada contínua que beneficia toda a comunidade escolar.

Guia de Segurança da Informação para

PROFESSORES

SEGURANÇA DIGITAL
EDUCAÇÃO DO PARANÁ

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO